MASTER EN SCIENCES INFORMATIQUES

Extensions à apporter au réseau Astrid et plus généralement à un réseau Tetra pour faire de la géolocalisation de personnes

Grawet, Laurent

Award date:
2007

Facultés Universitaires Notre-Dame de la Paix
Institut d'Informatique

Extensions à apporter au réseau ASTRID et plus généralement à un réseau TETRA pour faire de la géolocalisation de personnes

Laurent Grawet

Mémoire présenté en vue de l'obtention
du grade de Licencié en Informatique

Année Académique 2006 - 2007

Résumé

L'objectif de ce travail est de proposer une solution de géolocalisation de personnes au travers du réseau ASTRID et plus généralement des réseaux TETRA. ASTRID est un réseau numérique, dédié aux professionnels du secours et de la sécurité, implémentant la norme TETRA. Cette norme jouit d'une popularité grandissante en Europe et dans le monde, particulièrement dans le domaine des réseaux numériques professionnels.

De nombreuses applications sont possibles, mais l'étude est menée sur la surveillance électronique de condamnés, en raison des contraintes élevées illustrant bien ce système de géolocalisation.

La première étape consiste à réaliser un état de l'art sur le réseau, la norme et les techniques de géolocalisation. Viennent ensuite la définition des spécifications et la conception de l'architecture. Nous voyons également comment adapter et étendre le protocole LIP pour le rendre compatible avec les exigences du système. Finalement, les problèmes relatifs à la sécurité sont abordés avec une approche spécifique aux réseaux de géolocalisation.

Abstract

The objective of this paper is to propose a people location solution throughout the ASTRID network and, more generally, TETRA networks. ASTRID is a digital network, devoted to rescue and security professionals, implementing the TETRA norm. This norm has a growing popularity in Europe and the rest of the world, particularly in the field of dedicated digital networks.

There are numerous possible applications, but the study focuses on sentenced offenders placed under electronic surveillance, because of the high constraints that well illustrate the location system.

The first step consists to achieve the state of the art in network, norm and location techniques. Then come the specification and architecture conception. We also see how to adapt and extend the LIP protocol to make it compatible with the system requirements. Finally, security problems are discussed with a specific location network approach.

Remerciements :

Je remercie Monsieur Ramaekers, mon promoteur, pour sa disponibilité, sa patience et ses conseils avisés pendant l'élaboration de ce mémoire.

Merci à Laurent Schumacher pour son apport et ses conseils aidant à la réalisation de ce travail.

Je remercie également John Pyrgies pour ses informations et sa documentation. Je lui souhaite bonne continuation pour la fin de sa thèse.

Par ailleurs, je remercie l'ensemble du corps professoral et facultaire de la licence en informatique à horaire décalé. Puisse cette initiative indispensable vivre encore de longues années.

Je remercie ma famille et mes amis pour leur soutien et leurs encouragements.

Table des matières

Abréviations

3GPP 3rd Generation Partnership Project

A-GPS Assisted GPS

ASTRID All-round Semi-cellular Trunking Radio communication system with Integrated Dispatchings

AVL Automatic Vehicle Location

CCK Common Cipher Key

CP Clé Principale

CS Clé de Service

DCK Derived Cipher Key

DGPS Differential GPS

DQPSK Differential Quaternary Phase Shift Keying

EGNOS European Geostationary Navigation Overlay Service

ESA European Space Agency

ETSI European Telecommunications Standards Institute

FC Flux de Clés

GCK Group Cipher Key

GFC Génération de Flux de Clés

GLONASS GLObal'naya NAvigatsionnaya Sputnikovaya Sistema, qui signifie Système GLObal de NAvigation par Satellite

GPS Global Positioning System

ITSI Individual TETRA Subscriber Identity

K authentication Key

KS, KS' Session authentication Key

LIAISON LocatIon bAsed servIceS for the enhancement of wOrking enviroNment

LIP Location Information Protocol

LCS LoCation Services

M Message

MC Message Chiffré

MGCK Modified Group Cipher Key

RANDx RANDom challenge x

RESx RESponse x

RFID Radio Frequency Identification

RRLP Radio Ressource LCS (Location Services) Protocol

RS Random Seed

PDU Packet Data Unit

SA Selective Availability

SCK Static Cipher Key

SCORE Service of Coordinated Operational Emergency & Rescue using EGNOS

SDS Short Data Service

SIM Subscriber Identity Module

SNDCP SAP SubNetwork Dependent Convergence Protocol Service Access Point

SwMI Switching and Management Infrastructure

TA TETRA Algorithm

TDMA Time Division Multiple Access

TDOA Time Difference of Arrival

TETRA TErrestrial Trunked RAdio

VI Vecteur d'Initialisation

VS Valeur de Synchronisation

WAAS Wide Area Augmentation System

XRESx eXpected RESponse x

Introduction générale

Dans le dictionnaire des néologismes du ministère français de la Culture et de la Communication, on trouve la définition du terme « géolocalisation par satellite ». Il s'agit de la « Détermination de la position d'un point à la surface ou au voisinage de la Terre, par traitement des signaux radioélectriques en provenance de plusieurs satellites artificiels, reçus en ce point. »

Voici une seconde définition, donnée par le grand dictionnaire terminologique de l'Office québécois de la langue française : « géolocalisation n. f. Dans le contexte de l'utilisation d'appareils mobiles, comme les téléphones cellulaires, ensemble des techniques qui permettent de déterminer leur position géographique, à partir des ondes radio qu'ils émettent. »

Ces deux définitions apparaissent plutôt complémentaires, la seconde n'étant pas spécifique à la localisation par satellite. C'est justement cette nuance importante qui correspond bien au système qui sera présenté dans les chapitres suivants.

Quels sont les domaines visés par ce système de géolocalisation de personnes ? De par le type de réseau utilisé, il sera naturellement orienté vers les professionnels des secours et de la sécurité. Les applications sont multiples. Par exemple, le système pourrait servir à localiser les pompiers précisément dans un bâtiment ou dans de grandes étendues telles qu'une raffinerie. Les plans fournis par la ville permettraient une représentation en 3D de la position des hommes présents sur le terrain.

Une autre application, médicale cette fois-ci, servirait à contrôler les constantes biologiques de patients avec leur consentement. On pense ici immédiatement à des pathologies telles que les maladies cardio-vasculaires. Par exemple, un implant couplé ou intégré au stimulateur cardiaque serait activé en cas de trouble et donnerait des informations sur la position géographique du patient et ses constantes vitales.

Dans le même ordre d'idées, les personnes âgées, isolées, souffrant d'Alzheimer pourraient également bénéficier d'un tel système.

Une autre application possible consiste en une amélioration des dispositifs actuels de surveillance de condamnés. En Belgique, la surveillance électronique est actuellement réglementée par la circulaire ministérielle n° 1746bis du 26 novembre 2002 [1] [2].

Il est possible pour des condamnés dont les peines répondent à des critères précis, de bénéficier de la surveillance électronique comme modalité d'application d'une peine privative de liberté. Si la décision d'accorder la modalité au condamné est prise, le ministère de la Justice détermine l'emploi du temps à respecter par ce dernier. Cette description comporte une ou plusieurs périodes détaillées où sont spécifiées les activités professionnelles, formatrices, psychosociales et de loisir.

Le condamné sera porteur d'un bracelet de cheville électronique. Ce dispositif permet de surveiller et de vérifier le respect par le condamné des plages horaires précédemment définies. La liberté du condamné se voit ainsi librement restreinte, sa présence est requise en des lieux et à des endroits précis. Les vérifications sont effectuées par le Centre national de surveillance électronique (CNSE).

C'est ce cas de figure, comportant des contraintes élevées, qui va nous servir pour définir le système. En effet, il sera plus facile d'adapter le système pour une application avec des exigences plus légères que l'inverse.

Le dispositif actuel permet uniquement de savoir si le détenu muni de son bracelet est dans le périmètre du boîtier récepteur situé à son domicile. L'objectif est donc de proposer un système permettant la localisation précise des individus en tous temps et en tous lieux avec un temps de traitement minimal. La confidentialité des données sera également assurée.

Le mémoire se compose de quatre parties. Dans la première, un état de l'art sur le réseau et la norme utilisée ainsi que les techniques de localisation existantes sera réalisé.

La seconde partie introduira les spécifications de notre système grâce au diagramme des cas d'utilisation et des descriptions de scénarios.

La troisième partie traitera de la conception de l'architecture au moyen de diagrammes de séquence et de la description des paquets du protocole de géolocalisation utilisé.

Enfin, la dernière traitera des aspects de la sécurité. Quels sont les risques

encourus ? De quelle nature sont les attaques possibles, peut-on les détecter et peut-on s'en protéger ? Le présent document traite de la sécurité à partir du dispositif de géolocalisation jusqu'au serveur de suivi, l'aspect sécurisation des bases de données ne sera pas abordé.

Première partie

État de l'art

Introduction

Après une description du réseau ASTRID, des services offerts et de son infrastructure, nous parlerons de la norme TETRA sur laquelle ce réseau est basé. Suivra ensuite le protocole de localisation LIP adapté au réseaux TETRA ainsi que les différentes techniques de positionnement (GPS, DGPS, A-GPS...). Finalement, deux initiatives que sont les projets SCORE et LIAISON visant à développer et intégrer ces techniques dans les réseaux d'urgence ou commerciaux seront évoquées.

Chapitre 1

Le réseau ASTRID

ASTRID [3] qui est l'acronyme de *« All-round Semi-cellular Trunking Radio communication system with Integrated Dispatchings »* est un opérateur télécom dédié à tous les services belges de secours et de sécurité.

L'objectif d'ASTRID est de proposer un système de communication centralisé à l'ensemble des acteurs via un opérateur unique. Les professionnels du secours et de la sécurité sont confrontés à différents problèmes de communication depuis bon nombre d'années.

Les raisons sont entre autres l'utilisation de fréquences et de matériel différents ainsi que la capacité limitée des réseaux analogiques. Des centaines de petits réseaux répartis sur tout le territoire, différents pour chaque discipline, rendent difficile toute forme de communication.

Les catastrophes telles que les inondations ont permis de mettre en évidence les limites des réseaux analogiques existants, rapidement saturés, entraînant de grandes difficultés pour la coordination des différents services sur le terrain. A cela s'ajoute le problème de la confidentialité de l'information, les moyens actuels n'étant absolument pas protégés contre l'écoute illicite.

Le gouvernement belge a donc opté pour un réseau commun à l'ensemble des services de secours et de sécurité et c'est ainsi qu'ASTRID a vu le jour le 31 juillet 1998. Son capital est financé à 61% par l'état fédéral et à 39% par le holding communal. ASTRID, société anonyme de droit public, a été créée en exécution de la loi du 8 juin 1998 relative aux radiocommunications des services de secours et de sécurité. Les statuts sont établis par l'arrêté royal du 27 juillet 1998 délibéré en conseil des ministres. Ce réseau numérique repose sur le standard européen TETRA [4] de l'ETSI [5] adapté aux services de

secours et de sécurité.

1.1 Les services

Les 3 services du réseau ASTRID sont : radiocommunication, sémaphonie et dispatching. Il peuvent être utilisés indépendamment ou combinés en fonction des besoins. Le réseau permet la gestion de groupes de communication, c'est-à-dire la création dynamique de groupes de personnes qui doivent pouvoir communiquer en fonction de leur mission. Le système de sémaphonie permet de transmettre un message alphanumérique et/ou sonore à un destinataire situé en Belgique. Enfin, la position des équipes sur le terrain ainsi que leurs destinations sont déterminées en permanence via le service AVL *« Automatic Vehicle Location »*.

Actuellement, le système AVL est composé d'une radio TETRA sur laquelle est connecté un récepteur GPS. Les données sont ensuite transmises sous forme de messages SDS *« Short Data Service »* qui permettent à une application d'échanger régulièrement des informations avec l'infrastructure TETRA. L'affichage de ces données peut ensuite se faire sur une carte dans un centre de dispatching disposé dans chaque province ainsi qu'à Bruxelles. Ces centres informatisés, reliés aux réseaux de radiocommunication et de téléphonie permettent de suivre, guider et assister les interventions des différents services de secours et de sécurité.

Finalement, ASTRID transmet les communications vocales et de données en toute sécurité. Le chiffrement des communications numériques et l'authentification des terminaux garantissant un niveau de sécurité élevé.

1.2 L'infrastructure en bref

- Environ 500 antennes radio sur l'ensemble du territoire. Celles-ci remplaceront à terme les 1 500 antennes analogiques existantes.
- 40 000 terminaux potentiels sur le réseau.
- 11 centres de dispatching provinciaux.
- L'ASTRID Service Center (ASC) : monitoring technique 24/24, 7 jours sur 7 pour une sécurité et une disponibilité maximales.

FIG. 1.1 – L'infrastructure ASTRID

1.3 La norme ETSI TETRA

TETRA [4] est l'acronyme de *« TErrestrial Trunked RAdio »* et est une norme de l'ETSI [5] pour les radiocommunications professionnelles de voix et de données. La modulation de phase différentielle $\Pi/4$ DQPSK *« Differential Quaternary Phase Shift Keying »* est utilisée autorisant un débit de 18 000 symboles/sec. Chaque symbole correspond à 2 bits. TETRA utilise le système TDMA *« Time Division Multiple Access »* permettant quatre canaux utilisateurs sur une seule porteuse. Les porteuses sont quant à elles espacées de 25 kHz. La norme défini deux modes de communication :

Le mode « trunking » est un mode point à multipoint où les utilisateurs sont reliés à l'infrastructure TETRA. Ce mode comprend la gestion de groupes de discussion ainsi qu'une allocation dynamique de fréquences, en fonction des besoins, procurant une meilleure gestion des ressources. L'utilisateur n'a donc pas à se soucier de la gestion des fréquences ce qui lui permet de se focaliser à 100% sur sa mission.

Le mode « direct » est un mode point à point qui autorise une liaison directe entre les utilisateurs sans passer par le réseau. Cela permet notamment aux utilisateurs de communiquer entre eux en dehors de la

couverture du réseau (dans un sous-sol par exemple).

La norme permet la gestion de groupes de communication et le transfert de données à faible débit. Les principaux avantages sont :

- Rapidité d'établissement de la liaison, de l'ordre de la demi seconde pour un appel de groupe.
- Les modes alternatifs de fonctionnement tels que par exemple, le fait qu'une station fixe TETRA soit en mesure d'assurer les appels locaux en l'absence du reste du réseau. Ou encore, les liaisons directes entre mobiles, utiles lorsque le réseau est hors d'atteinte.
- Le mode passerelle où un mobile ayant accès au réseau peut servir de relais à d'autres mobiles qui ne sont pas en contact avec l'infrastructure.
- La confidentialité et la sécurité au travers l'authentification des utilisateurs et le chiffrement des communications vocales et de données.
- L'interopérabilité des systèmes, c'est-à-dire la communication transfrontalière (roaming).
- Un standard ouvert supporté par différents fabricants de matériel de transmission.

1.4 Le protocole LIP

LIP [6] est l'acronyme de « Location Information Protocol » et est également une norme de l'ETSI [5]. Il s'agit d'un protocole de couche applicative de géolocalisation, optimisé pour les interfaces mobiles TETRA. Ce dernier peut utiliser différents modes de transport tels que SDS *« Short Data Service »* ou SNDCP SAP *« SubNetwork Dependent Convergence Protocol Service Access Point »*. Le rapport de localisation peut être émis automatiquement sous contrainte d'événements ou par interrogation directe.

Chapitre 2

Les techniques de positionnement

2.1 GPS

Le GPS [7] ou « Global Positioning System » est le principal système de positionnement mondial par satellite actuel et c'est, de plus, le seul à être entièrement opérationnel.

Grâce à un système d'horloge atomique équipant les satellites, un récepteur GPS captant au moins quatre satellites peut connaître la distance le séparant de ces derniers en mesurant les écarts relatifs entre les horloges. Il peut ensuite calculer par trilatération sa position dans l'espace en trois dimensions. Ce système, mis en place par la défense américaine, possède une précision théorique de 15 mètres.

Malheureusement, l'armée américaine, concernée par le risque potentiel qu'un tel système puisse servir à des forces étrangères pour guider des systèmes d'armement, décida d'en réduire la précision. Et c'est ainsi que le système SA pour « *Selective Availability* » vu le jour, ramenant la précision à 100 mètres.

Il était toujours possible de bénéficier de la précision maximale si l'utilisateur était en possession des clés de déchiffrement mais cela réduisit significativement l'utilisabilité pour les usages non militaires. Après plusieurs années de pression, les opérateurs du réseau GPS ont accepté de déconnecter le SA en 2000.

Il convient également de parler de Galileo [8] qui est le le nom du futur

système de positionnement par satellite européen. La mise en service initialement prévue pour 2008 est retardé en raison de désaccords stratégiques et financiers. Il serait actuellement question de la mi-2012 au plus tôt. La précision horizontale est inférieure à 4 m et verticale inférieure à 8 m pour le service gratuit. Le service commercial bénéficiera quant à lui d'une précision d'un mètre pouvant être ramenée à moins de 10 cm avec l'aide de stations au sol.

GLONASS est quant à lui le système russe lancé en septembre 1993 mais qui n'est plus complètement opérationnel en raison de la durée de vie limitée des satellites (2 - 3 ans) et des problèmes économiques du pays. Néanmoins, sa mise à niveau est en cours avec la coopération de l'Inde et le réseau devrait être à nouveau pleinement opérationnel en 2008. Sa précision horizontale est évaluée à 55 mètres et 70 mètres pour la précision verticale. Cependant un signal plus précis est mis exclusivement à disposition des militaires russes.

Beidou, le système chinois composé de trois satellites est opérationnel uniquement sur le territoire chinois et les régions limitrophes. La Chine est également associée au projet européen Galileo. La précision est d'environ une trentaine de mètres.

2.2 DGPS

Le système DGPS [9] pour « *Differential GPS* » fut développé afin de palier à la limitation du SA. Le principe est basé sur le fait qu'en des points voisins, les erreurs de mesures sont très semblables. Il suffit donc de transmettre à l'unité mobile DGPS, les fluctuations des mesures de positionnement relevées grâces à des stations au sol recevant les mêmes satellites. Le récepteur DGPS pourra ainsi corriger une grande partie des erreurs de mesures, qu'elles soient dues aux conditions de propagation des ondes radio ou à des fluctuations volontaires du signal émis.

Malgré l'arrêt du signal SA en 2000, les systèmes DGPS ont continué à évoluer afin de faire encore mieux que le système GPS. Les meilleures implémentations offrent une précision sous la barre des 10 cm.

EGNOS [10] pour *« European Geostationary Navigation Overlay Service »* est le DGPS européen développé par L'ESA, la Commission européenne et EUROCONTROL. Considéré comme le précurseur de Galileo, le système consiste en trois satellites géostationnaires et un réseau de sta-

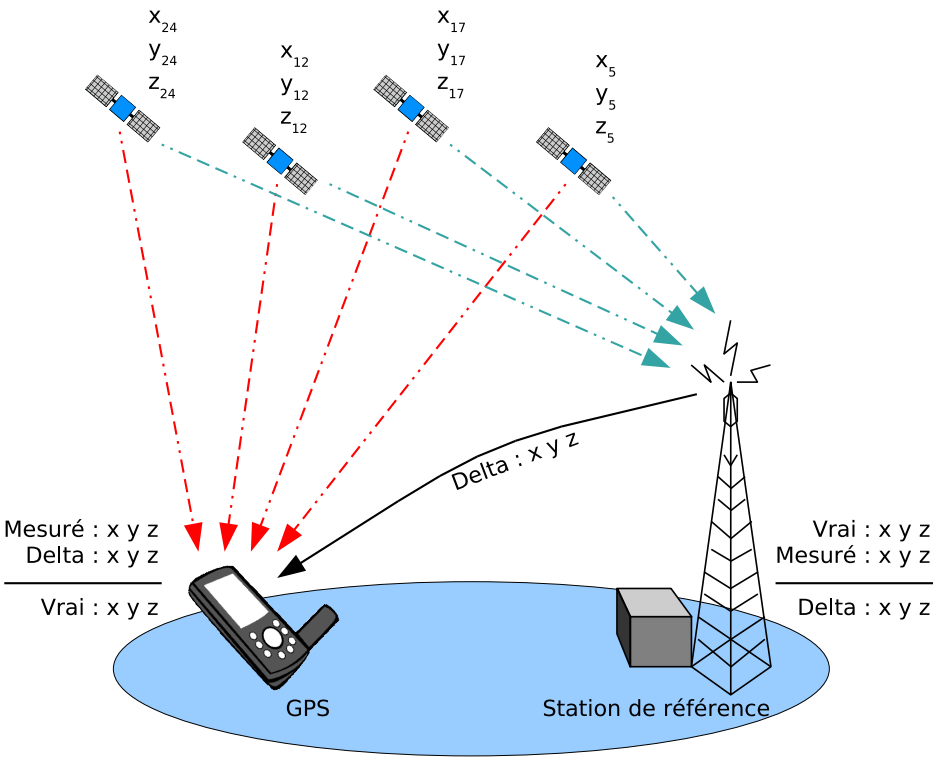

FIG. 2.1 – L'infrastructure DGPS

tions au sol. Ce dispositif vise à augmenter l'efficacité des systèmes GPS et GLONASS en émettant, au moyen de ces trois satellites, des informations sur la fiabilité et la précision des signaux de positionnement reçus. Cela permet aux utilisateurs de bénéficier d'une précision d'environ cinq mètres.

Le WAAS *« Wide Area Augmentation System »* est quant à lui le système DGPS opérationnel aux Etats-Unis.

2.3 AGPS

AGPS [11] pour *« Assisted GPS »* diffère du GPS traditionnel en ajoutant un élément supplémentaire à l'équation : un serveur d'assistance.

L'infrastructure est donc constituée de stations relais, d'un centre de commutation et d'un serveur. Comme le serveur connaît la position approximative du récepteur grâce au centre de commutation (cellule utilisée), il peut prédire quel signal GPS le récepteur recevra. Cette information est envoyée au récepteur par voie hertzienne au travers des relais.

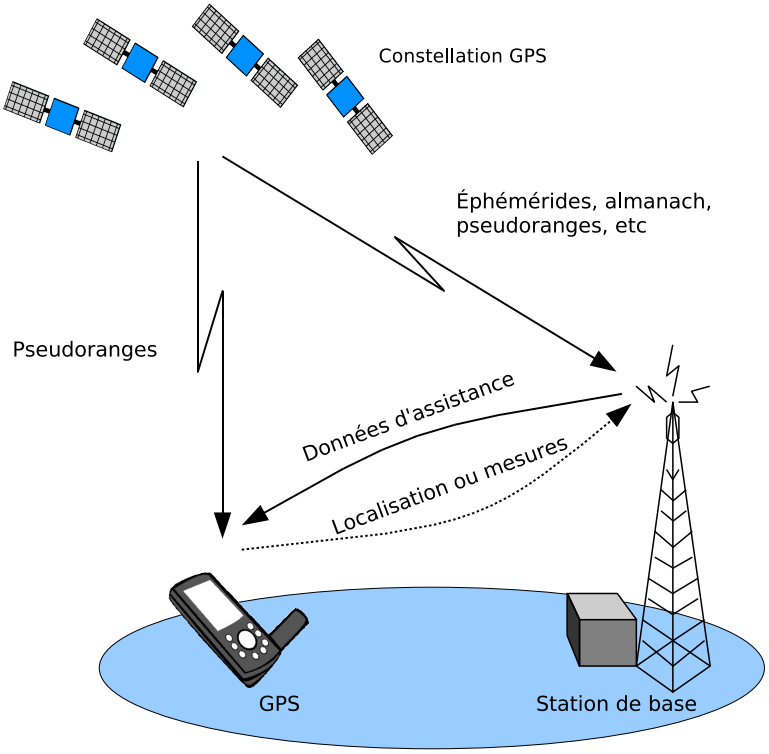

FIG. 2.2 – L'infrastructure AGPS

Grâce à la prédiction de ces informations, le temps d'initialisation du récepteur est largement réduit. La plupart des calculs de positionnement sont également réalisés par le serveur, l'unité mobile envoyant les données GPS à ce dernier.

Cette solution est particulièrement intéressante pour la localisation à l'intérieur des bâtiments, handicap du système GPS traditionnel. La précision est de l'ordre de 50 mètres en intérieur et 15 mètres à l'extérieur.

2.3.1 Le projet SCORE

SCORE [12], un consortium européen géré par Alcatel, étudie actuellement un procédé visant à améliorer la précision du système AGPS en le couplant avec une architecture DGPS telle que EGNOS. Cette étude se fait dans le cadre de la directive européenne E112 concernant la localisation des appels d'urgence ainsi que la localisation et le dispatching des équipes de secours. Le projet LIAISON contribue également au développement des techniques de localisation. L'objectif est de permettre :

- Une précision, disponibilité et couverture supérieure.
- Un temps d'initialisation du récepteur largement réduit.
- Une implémentation partielle du récepteur GPS dans l'unité mobile, la plupart des calculs étant effectués par le serveur.

Il en résulte une durée de vie de batterie accrue et un coût réduit dans la conception de l'unité mobile.

2.3.2 Le projet LIAISON

LIAISON [13] *« LocatIon bAsed servIceS for the enhancement of wOrking enviroNment »* est un autre consortium européen piloté par ALCATEL dont le but est de fournir des solutions de localisation aux professionnels de l'urgence.

Les problèmes actuellement rencontrés par les utilisateurs sont le manque de coordination entre les techniques de localisation et les radio mobiles, les faibles performances des techniques de localisation et le manque de synergie entre les acteurs.

Pour atteindre son objectif, LIAISON intégrera nombre de standards et techniques existants, proposant un ensemble de technologies avec la maturité requise pour une utilisation professionnelle.

Les principales techniques retenues sont EGNOS et Galileo pour la localisation associées aux derniers standards de télécommunication (GSM, UMTS, TETRA et WLAN).

2.4 Argos

Argos [14] est un système de localisation par satellite permettant de collecter les données environnementales de sujets fixes ou mobiles, de les traiter et de les diffuser à l'aide de centres de traitement disséminés à travers le monde. Ces informations sont émises par les balises Argos. On entend par le mot balise, tout émetteur radio automatique compatible avec le système Argos.

Il est possible de transmettre les informations de capteurs couplés à l'émetteur (température d'un container, chocs, vibrations, humidité, émanations toxiques, explosion, fuite, pluviométrie, vitesse du vent, etc.). Les balises peuvent être embarquées sur des bateaux, accrochées à des bouées dérivantes, posées sur des volcans, etc. Grâce à leur grande miniaturisation,

elles peuvent également être placées sur des petits mammifères et sur des oiseaux.

Les satellites Argos sont placés sur une orbite polaire. En raison de ce type d'orbite, le nombre de passages varie entre 7 (équateur) et 28 (pôles). Le temps d'acquisition varie entre 8 et 10 minutes. La précision est de l'ordre de 150 m.

En fonctionnement depuis 20 ans, ce système a largement prouvé sa fiabilité, fournissant des données à la recherche et à la protection de l'environnement à l'échelle mondiale.

Deuxième partie

Spécifications

Chapitre 3

Géolocalisation, protocole

3.1 Introduction

Le réseau utilisé étant ASTRID, il conviendra de déterminer comment la précision et la disponibilité de l'information de positionnement des personnes surveillées peuvent être améliorées (particulièrement à l'intérieur des bâtiments). Ceci, grâce à des technologies telles que le GPS différentiel (DGPS) ou le GPS assisté (AGPS). Ce chapitre établira en outre les modifications à apporter au réseau actuel pour supporter ces technologies (DGPS, AGPS) si elles s'avèrent utiles.

Le choix du protocole de communication se fera en fonction des contraintes du système et des éléments existants sur le réseau ASTRID.

3.2 Traqueur

La personne mise sous surveillance électronique sera porteuse, au poignet ou à la cheville, d'un dispositif de géolocalisation personnel : le traqueur. Cet appareil, muni d'un récepteur GPS minimal, sera relié à l'infrastructure TETRA au moyen d'un émetteur/récepteur radio intégré, opérationnel sur la bande de fréquences UHF 380 - 400 Mhz (spécifique au réseau ASTRID).

Le serveur de localisation AGPS relié à l'infrastructure TETRA pourra, sur base des cellules du réseau à portée du traqueur, effectuer une première localisation par TDOA *« Time Difference of Arrival »*. Cette technique consiste à mesurer les écarts de temps entre l'émission du signal et sa réception dans minimum trois sites.

Grâce à ces informations, le serveur sera en mesure de récupérer les données d'assistance GPS de la station recevant les mêmes satellites que le traqueur. Il retournera ensuite ces données au traqueur qui pourra ainsi se verrouiller rapidement sur les satellites GPS et recevoir leurs « *Pseudo Random Noise* » (PRN) codes. Les mesures GPS seront alors retournées au serveur de localisation qui effectuera les calculs nécessaires.

L'émission des données de localisation par le traqueur se fera après l'écoulement d'un timer fixant l'intervalle minimum entre deux émissions. En cas de déplacement du porteur, l'émission se fera à chaque $\triangle d$ (distance) déterminé, avec un nombre maximum d'envois par minute. A chaque envoi de données, le timer sera remis à 0. Il sera également possible de commander manuellement l'émission de données de localisation d'un traqueur particulier au travers l'infrastructure TETRA.

La confidentialité des informations de positionnement sera garantie par par le chiffrement des données.

3.3 Implant

Afin d'augmenter la sécurité du traqueur, il pourrait par exemple être couplé à un implant RFID *« Radio Frequency Identification »* sur le porteur du traqueur [15]. Ce circuit aurait une implémentation TETRA et LIP minimale. Si le porteur se séparait du traqueur ou l'endommageait, l'implant émettrait alors un signal d'alarme sur le réseau. L'implant serait également équipé d'un circuit Argos représentant la dernière chance pour localiser le condamné.

Le dispositif aurait la forme d'un cylindre de deux centimètres de long et d'un centimètre de diamètre [15]. Il serait implanté profondément sous la peau ou dans l'abdomen au moyen d'une intervention chirurgicale légère, réalisée par un chirurgien qualifié.

FIG. 3.1 – L'implant RFID de VeriChip

Cette technologie peut paraître avant-gardiste et soulève de nombreuses questions éthiques, qui ne seront pas débattues ici en raison de leur com-

plexité nécessitant une étude à part entière.

On peut cependant souligner que des implants (VeriChip) sont déjà utilisés dans des situations bien plus légères, telles que des discothèques célèbres de Rotterdam et de Barcelone. L'implant permet au client de régler ses consommations en passant son bras à proximité d'une borne. De manière surprenante, le succès est important comme en témoignent les listes d'attente.

L'implant n'est pas indispensable à notre application mais constitue une sécurité supplémentaire non négligeable. Son implantation sera d'autant plus aisée que sa taille diminuera grâce aux avancées technologiques. La conception tiendra donc compte de l'implant mais il sera possible de s'en passer au prix de quelques modifications mineures.

3.4 Technique de géolocalisation et suivi

Notre application nécessite une précision de localisation assez élevée, moins d'une dizaine de mètres. De plus, la localisation doit être possible à l'intérieur de bâtiments, ce que la technologie GPS habituelle est incapable de faire. A cela s'ajoutent les contraintes imposées par le ou les dispositifs portables du détenu.

A la vue de ces exigences, la technologie A-GPS permet de satisfaire à celle de la couverture à l'intérieur des bâtiments et aux contraintes matérielles (puissance de calcul, batteries...) des dispositifs portables. Cette technologie couplée à celle du DGPS permettra d'obtenir la précision souhaitée.

Le réseau ASTRID n'a pas d'infrastructure spécifique pour ces technologies, la technique utilisée actuellement étant celle du GPS (voir 1.1 page 6). Il conviendra donc d'installer un serveur de localisation couplé à des stations DGPS de référence. Si le serveur A-GPS fera partie de l'infrastructure (particulièrement pour des raisons de confidentialité de données), il sera par contre possible de le coupler à un système DGPS existant tel que EGNOS.

Un serveur de suivi sera responsable du stockage des données de géolocalisation. Il sera possible de connaître la position des sujets à chaque instant ainsi que d'obtenir un historique de leurs déplacements. Vu le caractère privé des données, des mesures de sécurité adéquates devront être prises.

3.5 Réseau et protocole

Le choix du réseau ASTRID n'est pas anodin. Les applications auxquelles le système est destiné nécessitent une haute disponibilité du réseau. Cette contrainte n'est pas respectée sur les réseaux de téléphonie mobile standards. Il suffit de constater la saturation des relais à proximité d'un embouteillage causé par un accident sur l'autoroute, lors de grands événements (festivals et fêtes) ou encore, la surcharge de l'entièreté des réseaux dans la nuit de la Saint-Sylvestre. Dans ce cas précis, les opérateurs vont jusqu'à déconnecter certains services afin de tenter de palier au dépassement de capacité.

Pour des événements localisés et planifiés, les gestionnaires des réseaux peuvent compenser la surcharge en installant des relais mobiles temporaires. Mais que se passera-t-il en cas d'événements imprévus tels que des accidents ou catastrophes ?

Il est important de noter que le service n'est également pas garanti en cas de dysfonctionnement d'éléments du réseau. ASTRID possède quant à lui un centre de monitoring technique actif en permanence. Ce centre effectue également des mesures de capacité et de performance nécessaires afin de garantir la qualité et la capacité du réseau à long terme.

L'équipement de transmission est également testé et évalué par les ingénieurs d'ASTRID afin de garantir les meilleures conditions de fonctionnement, la qualité de conception (résistance aux chocs...) et une utilisation intuitive. Les appareils sont testés pendant plusieurs semaines en laboratoire, sur bancs d'essai ainsi que sur le terrain.

De par son intégration à la norme TETRA, le protocole LIP semble être le choix adéquat. Il y a malgré tout un petit bémol : il n'est pas adapté aux techniques de localisation avancées telles que l'A-GPS. L'ETSI est cependant en train de définir une nouvelle norme [16] mais celle-ci ne sera pas disponible avant plusieurs mois. Il sera donc nécessaire d'ajouter cette nouvelle fonctionnalité au protocole dans la phase de conception. Le caractère sensible des données véhiculées impose que le protocole soit sécurisé.

3.6 Architecture réseau

L'architecture du réseau est illustrée à la figure 3.2. On peut constater qu'à l'instar du traqueur et de l'implant, le centre de suivi et le serveur A-

GPS sont reliés à l'infrastructure TETRA via un réseau câblé. Le serveur de suivi est également en liaison avec un centre Argos lui fournissant, si nécessaire, les informations de localisation en provenance des implants.

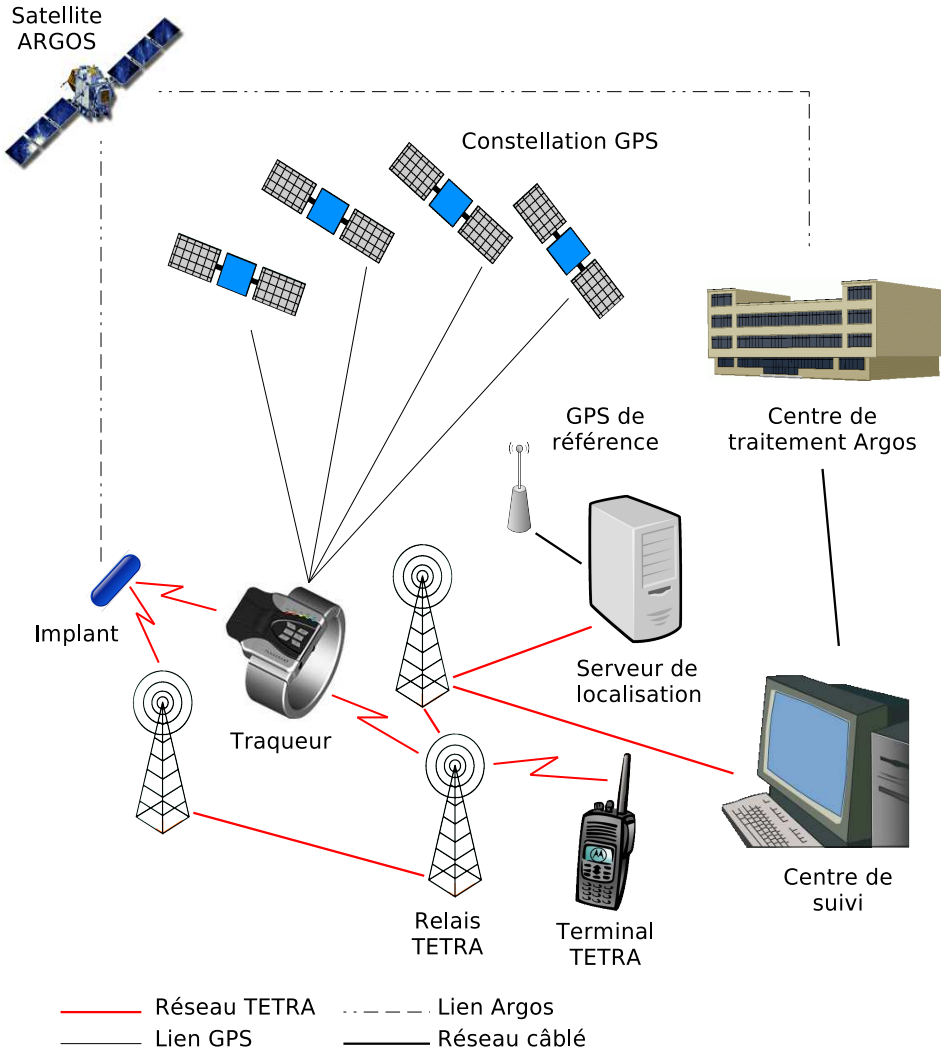

FIG. 3.2 – Architecture réseau

3.7 Conclusion

L'architecture proposée comporte cinq nouvelles entités qui permettent de collecter et de traiter les données en provenance du traqueur et de l'implant ansi que de fournir des informations de positionnement :

- la constellation Argos,
- le centre de traitement Argos,
- le serveur de localisation,
- les stations GPS de référence,
- le serveur de localisation.

Dans le cas de la surveillance de condamnés, le serveur de suivi peut être intégré au Centre national de surveillance électronique (CNSE) et donc être externe à l'infrastructure ASTRID. Il en va de même pour le serveur de localisation. Une possibilité consiste alors à faire transiter TETRA au dessus de la couche réseau IP (TETRA over IP).

Chapitre 4

Spécification des exigences fonctionnelles

4.1 Introduction

La méthodologie utilisée est celle des cas d'utilisation telle que spécifiée par la norme UML. Elle va permettre de capturer et de décrire les exigences fonctionnelles du système.

Nous considérons le traqueur et l'implant comme acteurs et donc extérieurs au système. Cela peut paraître surprenant au premier abord, mais correct en raison de la nature imprévisible du comportement du porteur.

4.2 Vérifier présence implant

Résumé Le traqueur vérifie la présence de l'implant créant ainsi un lien « discret » à courte distance.

Acteurs Le traqueur et l'implant

Dépendance Le cas d'utilisation « Envoyer résultat vérification implant »

Pré-condition Le traqueur est opérationnel.

Flux de base

1. Le traqueur envoie une requête à l'implant lors de sa mise en fonction et ensuite à intervalles réguliers de manière à vérifier sa présence.
2. Inclure le cas d'utilisation « Envoyer résultat vérification implant ».

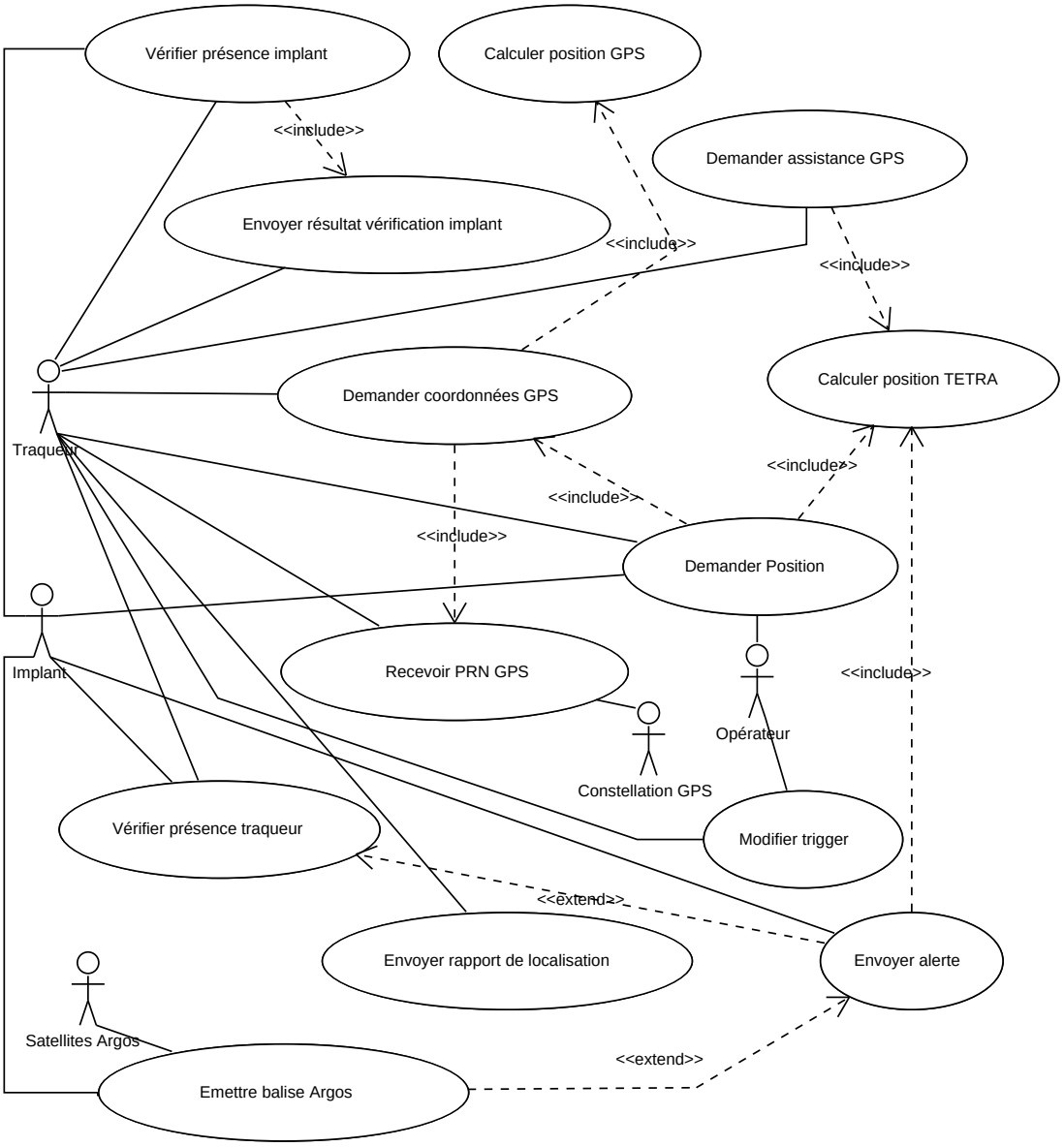

FIG. 4.1 – Diagramme des cas d'utilisation

3. Fin du cas d'utilisation.

Post-condition Le traqueur a déterminé si l'implant est présent et envoyé le résultat au serveur de suivi.

4.3 Envoyer résultat vérification implant

Résumé Le traqueur envoie au centre de suivi le résultat de la vérification de présence de l'implant.

Acteur Le traqueur

Dépendance Néant

Pré-condition Le traqueur est opérationnel et l'infrastructure TETRA est disponible. Le serveur de suivi est disponible.

Flux de base

1. Le traqueur envoie au serveur de suivi, au travers de l'infrastructure TETRA, le résultat de la vérification de présence de l'implant.
2. Fin du cas d'utilisation.

Post-condition Le serveur de suivi est notifié du résultat de la vérification de la présence de l'implant.

4.4 Vérifier présence traqueur

Résumé L'implant vérifie la présence du traqueur lorsque l'attente d'une requête de vérification provenant du traqueur abouti à un timeout.

Acteurs Le traqueur et l'implant

Dépendance Néant

Pré-condition L'implant est opérationnel.

Flux de base

1. Lorsque l'implant n'a pas reçu de requête de vérification de présence en provenance du traqueur passé le délais défini, il envoie une requête afin de tenter de rétablir le lien discret les unissant.
2. Le traqueur répond.

3. L'implant désactive le mode « alerte ».
4. Fin du cas d'utilisation.

Post-condition L'implant a reçu une réponse du traqueur, le mode alerte est inactif.

4.5 Envoyer alerte

Résumé L'implant envoie une alerte au serveur de suivi car le traqueur n'a pas répondu.

Acteur L'implant

Dépendances Les cas d'utilisation « Vérifier présence traqueur » et « Calculer position TETRA »

Pré-condition L'implant est opérationnel et l'infrastructure TETRA est disponible.

Flux de base

1. Le cas d'utilisation commence au point 2 du cas d'utilisation principal « Vérifier présence traqueur ».
2. Le traqueur ne répond pas.
3. L'implant se place en mode « alerte ».
4. L'implant désactive le mode « Argos ».
5. L'implant émet un message d'alerte à destination du serveur de localisation.
6. Inclure le cas d'utilisation « Calculer position TETRA »
7. Le serveur de localisation transfère le message d'alerte ainsi que les coordonnées TETRA au serveur de suivi qui les enregistre.
8. Fin du cas d'utilisation.

Post-condition Le serveur de suivi a reçu l'alerte et les coordonnées TETRA de l'implant.

4.6 Émettre balise Argos

Résumé L'implant émet un signal de balise Argos.

Acteur L'implant

Acteur secondaire L'infrastructure Argos

Dépendance « Envoyer alerte »

Pré-condition L'implant est en mode « alerte » et/ou « Argos » et n'est pas à portée de l'infrastructure TETRA.

Flux de base

1. Le cas d'utilisation commence au point 4 du cas d'utilisation principal « Envoyer alerte ».
2. L'implant passe en mode « Argos ».
3. L'implant émet la balise Argos à intervalles réguliers.
4. Fin du cas d'utilisation.

Post-condition La balise Argos est émise à intervalles réguliers.

4.7 Calculer position TETRA

Résumé La position du traqueur ou de l'implant est déterminée par le serveur de localisation au moyen de TETRA.

Acteur Le traqueur ou l'implant

Dépendance Néant

Pré-condition Le serveur est opérationnel. L'implant et/ou le traqueur sont opérationnels et des données ont été reçues. Le réseau TETRA est opérationnel.

Flux de base

1. Le traqueur ou l'implant émettent des données.
2. La localisation du traqueur et/ou de l'implant est réalisée via le réseau TETRA par *« Time Difference of Arrival »* (TDOA) sur base des données émises par ces dispositifs.
3. Fin du cas d'utilisation.

Post-condition La position TETRA du traqueur ou de l'implant est connue du serveur de localisation.

4.8 Calculer position GPS

Résumé La position du traqueur est calculée par le serveur de localisation.

Acteur Le traqueur

Dépendance Néant

Pré-condition Le serveur est opérationnel. Le traqueur est localisé par TDOA.

Flux de base

1. Le traqueur envoie les mesures GPS au serveur de localisation au travers de l'infrastructure TETRA.
2. Grâce à la localisation TDOA, le serveur de localisation récupère les informations de correction auprès des stations DGPS.
3. Le serveur de localisation calcule la position GPS et applique les corrections en provenance des stations DGPS.
4. Fin du cas d'utilisation.

Post-condition La position GPS du traqueur est connue du serveur de localisation.

4.9 Demander assistance GPS

Résumé Le traqueur demande au serveur de localisation les données d'assistance GPS.

Acteur Le traqueur

Dépendance Le cas d'utilisation « Calculer position TETRA »

Pré-condition Le réseau TETRA, le serveur de localisation et le traqueur sont opérationnels.

Flux de base

1. Le traqueur effectue une demande de données d'assistance GPS au serveur de localisation.
2. Inclure le cas d'utilisation « Calculer position TETRA ».
3. Le serveur de localisation envoie au traqueur les données d'assistance.

4. Fin du cas d'utilisation.

Post-condition Les informations d'assistance GPS ont été envoyées au traqueur.

4.10 Recevoir PRN GPS

Résumé Le traqueur reçoit les « Pseudo Random Noise codes » de la constellation GPS.

Acteur Le traqueur

Acteur secondaire La constellation GPS

Dépendance Néant

Pré-condition Le traqueur est en mesure de recevoir les signaux de la constellation GPS.

Flux de base

1. Le traqueur reçoit les PRN.
2. Fin du cas d'utilisation.

Post-condition Le traqueur a reçu les PRN.

4.11 Demander coordonnées GPS

Résumé Le traqueur demande les coordonnées GPS au serveur de localisation.

Acteur Le traqueur

Dépendances Les cas d'utilisation « Recevoir PRN GPS » et « Calculer position GPS »

Pré-condition Le réseau TETRA, le serveur de localisation et le traqueur sont opérationnels.

Flux de base

1. Inclure le cas d'utilisation « Recevoir PRN GPS » . **[FA1]**
2. Inclure le cas d'utilisation « Calculer position GPS ».
3. Le serveur de localisation renvoie au traqueur les coordonnées GPS qui font également office d'accusé de réception.

4. Fin du cas d'utilisation.

Flux alternatif

FA1.

1. Si le traqueur n'est pas en mesure de recevoir les signaux de la constellation GPS, il se signale à intervalles réguliers au serveur de localisation par un rapport vide afin de permettre sa localisation par TDOA.
2. Inclure le cas d'utilisation « Calculer position TETRA ».
3. Le serveur de localisation envoie les coordonnées TETRA au serveur de suivi.
4. Fin du cas d'utilisation.

Post-condition Le traqueur a reçu les coordonnées GPS.

4.12 Envoyer rapport de localisation

Résumé Le traqueur envoie l'information de positionnement au centre de suivi.

Acteurs Le traqueur

Dépendance Néant

Pré-condition Les coordonnées GPS sont connues du traqueur. Le réseau TETRA, le traqueur et le serveur de suivi sont opérationnels.

Flux de base

1. Le traqueur envoie son rapport de localisation.
2. Le serveur de suivi envoie un accusé de réception et enregistre les coordonnées.
3. Fin du cas d'utilisation.

Post-condition Les informations de localisation sont connues du serveur de suivi.

4.13 Demander position

Résumé Un opérateur effectue une demande de localisation d'un traqueur au serveur de suivi, au moyen d'un terminal.

Acteurs L'opérateur, le traqueur et l'implant

Dépendances Les cas d'utilisation « Demander coordonnées GPS », « Envoyer rapport de localisation » et « Calculer position TETRA »

Pré-condition Le terminal TETRA, les serveurs de localisation et de suivi sont opérationnels. L'infrastructure TETRA est disponible. Le terminal est autorisé à demander la position du traqueur.

Flux de base

1. L'opérateur fait sa demande au serveur de suivi au moyen d'un terminal.
2. Le serveur de suivi fait une requête de signalement immédiat au traqueur. **[FA1]**
3. Inclure le cas d'utilisation « Demander coordonnées GPS ».
4. Inclure le cas d'utilisation « Envoyer rapport de localisation ».
5. Le serveur enregistre et transfère le rapport au terminal TETRA.
6. Fin du cas d'utilisation.

Flux alternatifs

[FA1]

1. Si le traqueur ne répond pas, le serveur de suivi fait sa demande à l'implant. **[SFA1]**
2. Inclure le cas d'utilisation « Envoyer alerte »
3. Inclure le cas d'utilisation « Calculer position TETRA ».
4. Le serveur de localisation envoie les coordonnées TETRA ou Argos (si disponibles) au serveur de suivi qui les enregistre.
5. Le terminal TETRA est notifié du problème par le serveur de suivi et les informations TETRA/Argos de l'implant lui sont envoyées.
6. Les dernières informations de positionnement disponibles du traqueur sont extraites de la base de données du serveur et envoyées au terminal.

7. Ensuite, retour au point 5 du cas d'utilisation principal.

Sous flux alternatif

[SFA1]

1. Si l'implant ne répond pas, le terminal TETRA est notifié par le serveur de suivi.
2. Les dernières informations de positionnement disponibles du traqueur et de l'implant sont extraites de la BD du serveur. Si ces informations ne sont pas disponibles, le terminal TETRA est notifié et le cas d'utilisation se termine.
3. Les informations TETRA/GPS du traqueur et TETRA/Argos de l'implant sont envoyées au terminal.
4. Ensuite, retour au point 5 du cas d'utilisation principal.

Post-condition Le terminal a reçu les dernières informations de localisation du traqueur et/ou de l'implant disponibles.

4.14 Modifier trigger

Résumé Un opérateur effectue une demande de modification de trigger sur le traqueur, au moyen d'un terminal.

Acteurs L'opérateur, le traqueur

Dépendance Néant

Pré-condition Le terminal TETRA, le serveur de suivi et le traqueur sont opérationnels, l'infrastructure TETRA est disponible. Le terminal est autorisé à modifier le trigger.

Flux de base

1. L'opérateur fait sa demande au serveur de suivi au moyen d'un terminal.
2. Le serveur de suivi transfère la demande au traqueur.
3. Le traqueur applique les paramètres et confirme au serveur de suivi.
4. Le serveur de suivi confirme au terminal.

5. Fin du cas d'utilisation.

Post-condition Le trigger est modifié et le terminal a reçu confirmation.

4.15 Conclusion

Les cas d'utilisation ont permis de mettre à jour les exigences fonctionnelles du système.

On remarquera que l'opérateur du terminal TETRA est bien acteur et non le terminal, ce dernier faisant partie du système. Cela peut paraître paradoxal par rapport au porteur du traqueur et de l'implant, mais il n'en est rien. En effet, l'opérateur a une action directe sur le terminal, c'est lui qui décide des opérations à réaliser, quand il souhaite passer en émission... Par opposition, le porteur du dispositif de géolocalisation a une action indirecte avec ce dernier, il ne fait qu'induire par son comportement le fonctionnement du dispositif.

Troisième partie

Conception

Chapitre 5

Diagrammes de séquence

Les cas d'utilisation du chapitre précédent nous permettent de déduire les diagrammes de séquence suivants. Ces diagrammes représentent le dialogue entre les différentes entités du réseau TETRA au moyen du protocole LIP.

Certains diagrammes sont un condensé de plusieurs cas d'utilisation de manière à en simplifier la représentation.

La description du contenu des paquets de données sera réalisée au chapitre suivant.

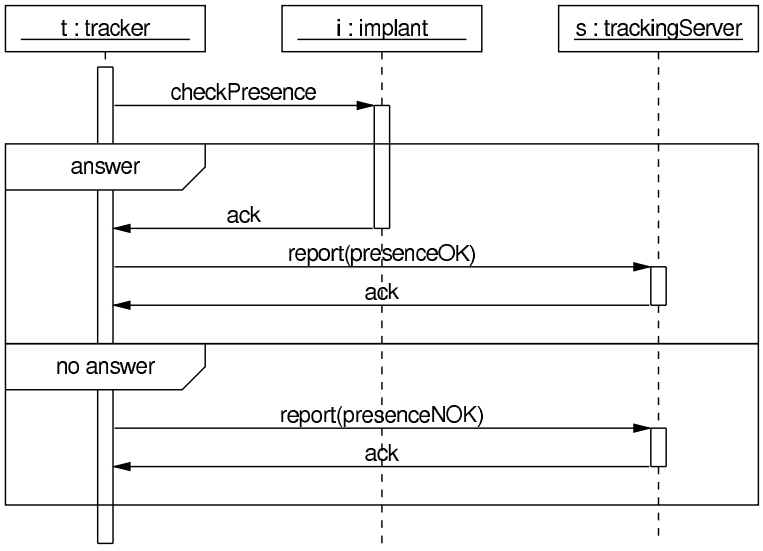

FIG. 5.1 – Vérifier présence implant

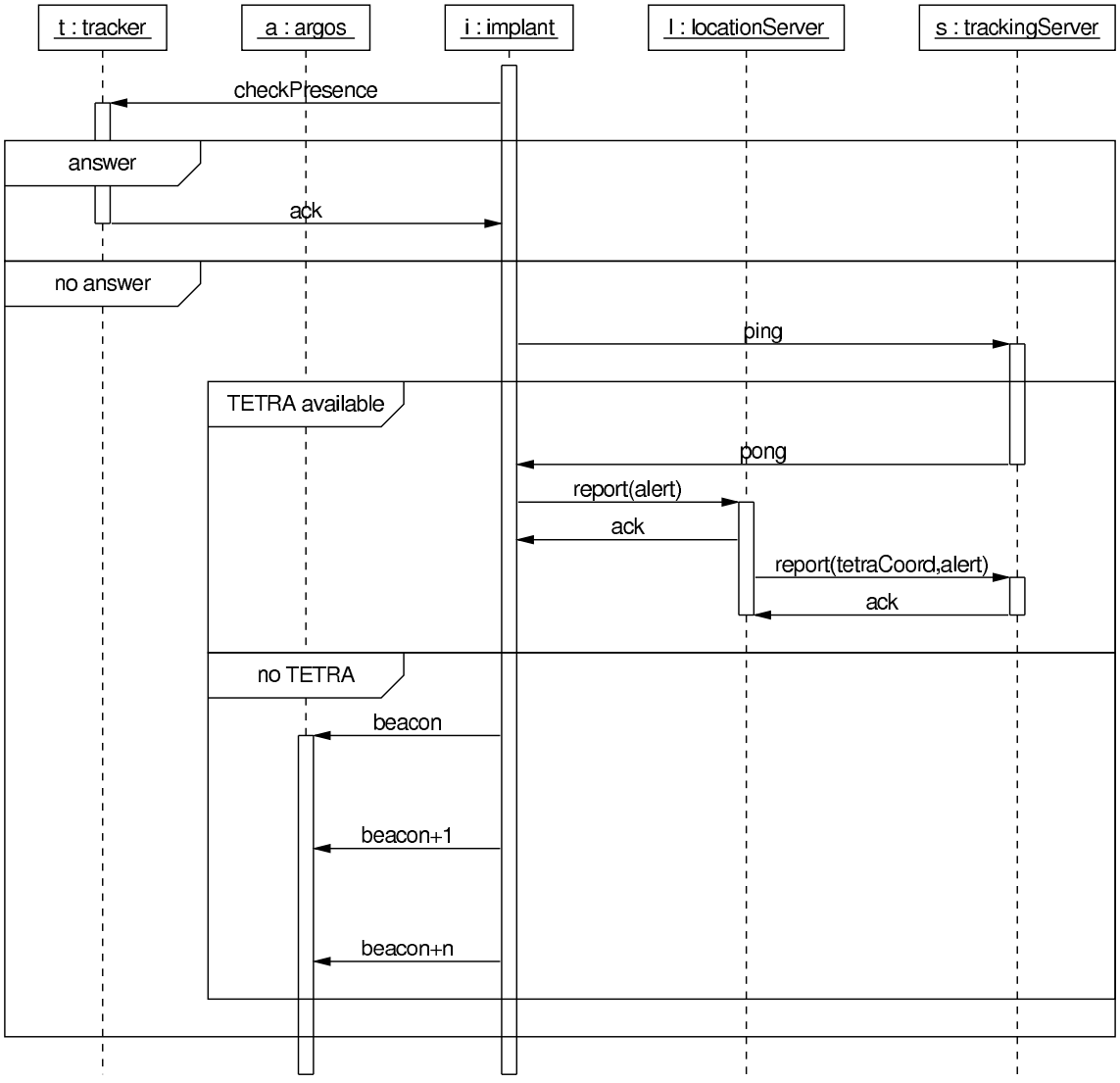

FIG. 5.2 – Vérifier présence traqueur

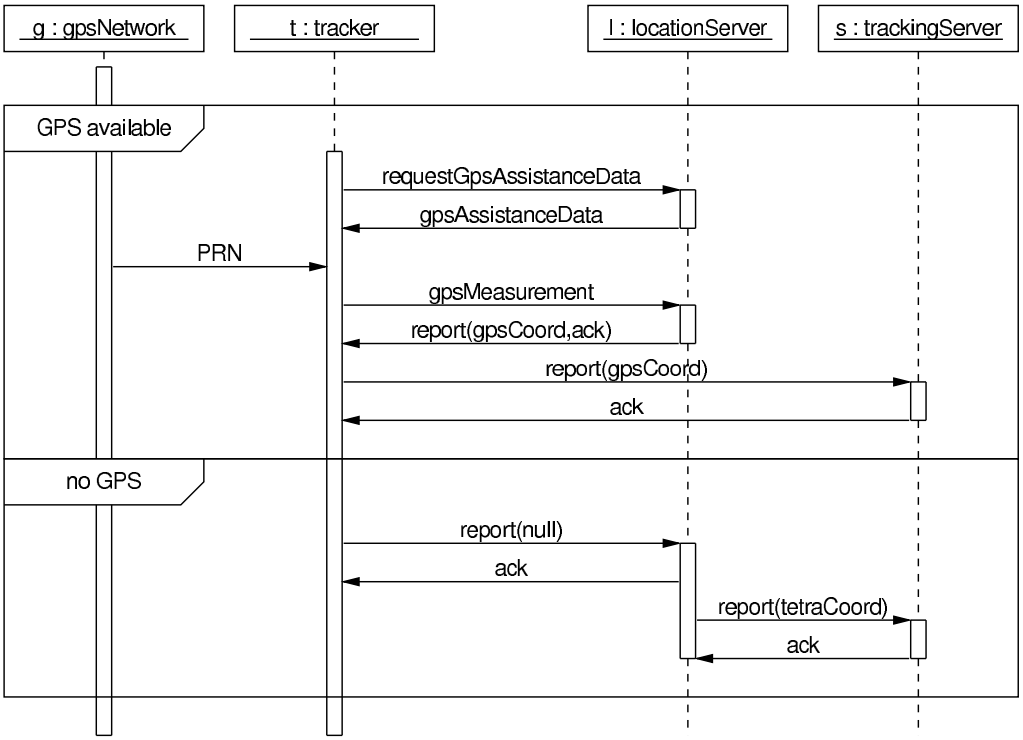

FIG. 5.3 – Rapport de localisation

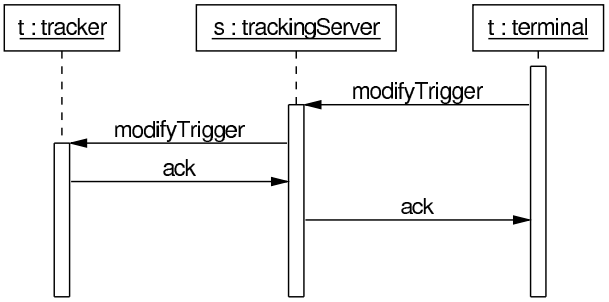

FIG. 5.4 – Modifier trigger

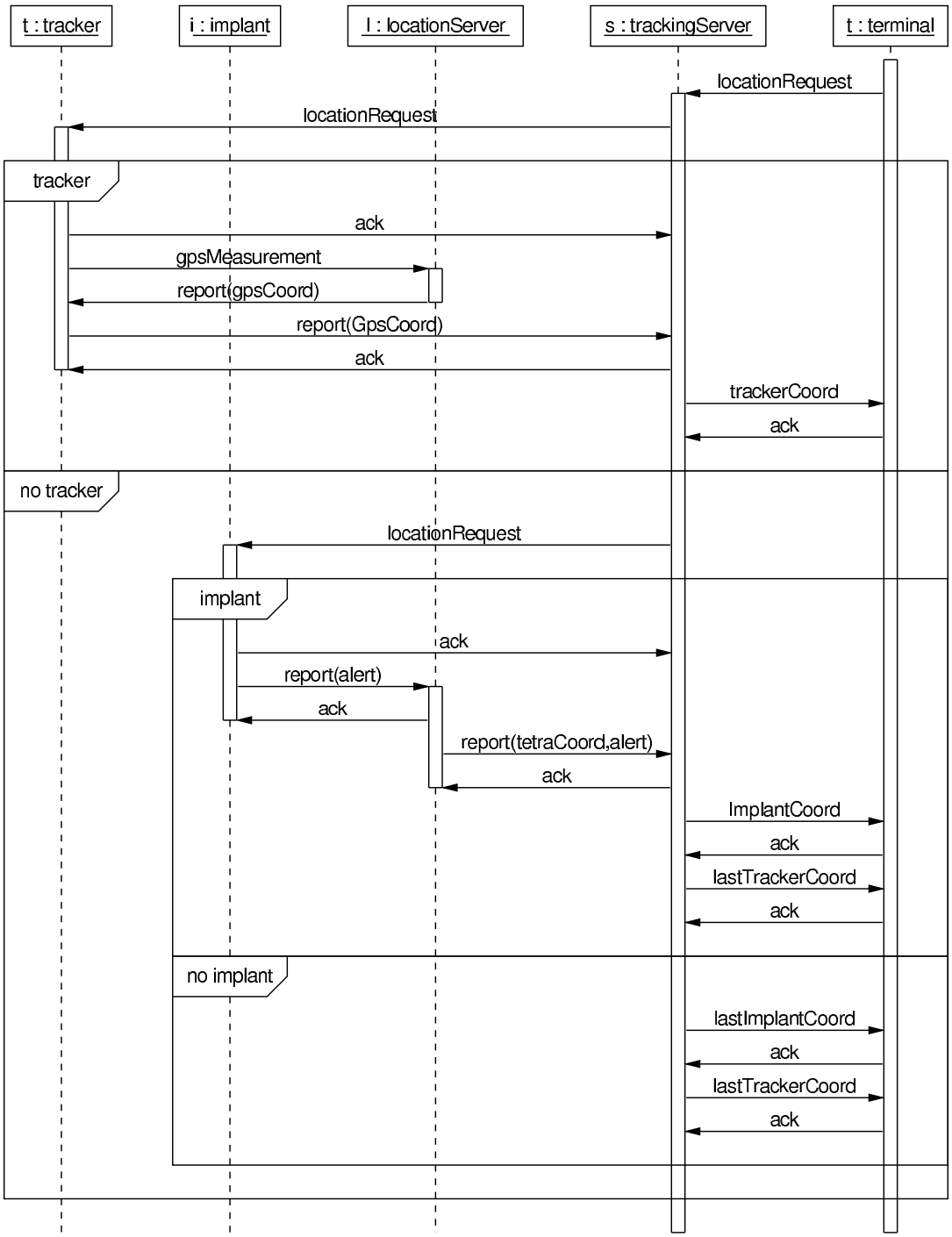

FIG. 5.5 – Demander position

Chapitre 6

Description des paquets

6.1 Introduction

Ce chapitre décrit le contenu des paquets échangés entre les entités comme illustré dans le chapitre précédent.

Nous verrons au point 6.3 comment pallier à l'absence du support A-GPS dans la norme LIP comme énoncé dans les spécifications au point 3.5 page 20.

6.2 Rapport de localisation

Voici dans le protocole LIP le paquet utilisé pour émettre un rapport de localisation. Il s'agit du *« Short location report »*.

Pour chaque paquet, une courte description des champs sera donnée[1]. L'unité de la colonne « length » est le bit. C/O/M indique si l'information est conditionnelle (dépend d'un autre champ), optionnelle, ou obligatoire.

Time elapsed : Représente le temps approximatif depuis la dernière détermination de position (< 5 s, < 5 min, < 30 min, pas disponible).

Longitude, latitude : La longitude et latitude.

Position error : L'incertitude de positionnement (2 m, 20 m, 200 m, 2 km, 20 km, 200 km, $>$ 200 km, inconnue).

Horizontal velocity : La vitesse de déplacement horizontal.

[1] Le lecteur pourra consulter les détails dans [6].

Information element	Length	Type	C/O/M	Value	Remark
PDU type	2	1	M	$[0]_2$	Short location report
Time elapsed	2	1	M		
Longitude	25	1	M		
Latitude	24	1	M		
Position error	3	1	M		
Horizontal velocity	7	1	M		
Direction of travel	4	1	M		
Type of additionnal data	1	1	M		
Reason for sending	8		C		See note 1
User defined data	8		C		See notes 1 and 2

NOTE 1 : This information element shall be present as defined by the Type of additional data information element.

NOTE 2 : The contents of this information element is outside the scope of the present document.

This PDU shall not include any O-bit in the coding as there will never be any optional information elements.

TAB. 6.1 – Short location report PDU (LIP)

Type of additionnal data : Détermine si le champ *« reason for sending »* ou *« user defined data »* sera utilisé.

Reason for sending : Indique la raison pour laquelle l'information a été émise depuis l'entité chargée de la localisation.

User defined data : Format libre, n'importe quelle valeur de 0 - 255.

Comme on peut le constater, les champs où se trouvent les informations de localisation dans ce paquet n'acceptent que des informations calculées et non des éléments de mesure GPS bruts.

6.3 Envoyer mesures GPS

Face à l'absence de support de l'A-GPS au sein de LIP, pourquoi ne pas étendre le protocole avec des éléments de normes existantes pour d'autres réseaux ? Il semble raisonnable de se porter sur des standards ouverts tels que ceux édités par le 3GPP [17]. Il s'agit d'un projet commun de différents organismes de standardisation en vue d'établir les spécifications techniques des réseaux de téléphonie mobile de $3^{ème}$ génération.

Le protocole qui nous intéresse est RRLP *« Radio Ressource LCS (Location Services) Protocol »*. Deux normes traitent des services de localisation au niveau de la station mobile [18] et de la station de base [19]. Les informations qui nous intéressent sont celles traitant de l'envoi des mesures GPS et des données d'assistance. Dans le tableau 6.2 nous retrouvons le format des données de localisation envoyées par le mobile vers le serveur dans un paquet RRLP. Une description détaillée de ces différents champs est disponible à l'annexe A page 79.

Information element	Length	Occurence	C/O/M	Resolution	Range	Unit
Reference Frame	16	1	O	—	1 - 65535	ms
GPS TOW	24	1	M	1 ms	0 - 14399999	ms
# of Satellites (N_SAT)	4	1	M	—	1-16	—
Measurement parameters	57	N_SAT	M	see tab. A.2		

TAB. 6.2 – GPS Measurement Information element content (RRLP)

Il ne reste plus qu'à remplacer les données de localisation du paquet LIP par les éléments de mesure GPS du protocole RRLP. Ceci nous donne le *« Short measurement report PDU »* du tableau 6.3.

Information element	Length	Type	C/O/M	Value	Remark
PDU type	2	1	M	$[10]_2$	Short measurement report
Time elapsed	2	1	M		
GPS Measurement info.	101 - 956	1	M		
Type of additionnal data	1	1	M		
Reason for sending	8		C		See note 1
User defined data	8		C		See notes 1 and 2

NOTE 1 : This information element shall be present as defined by the Type of additional data information element.

NOTE 2 : The contents of this information element is outside the scope of the present document.

This PDU shall not include any O-bit in the coding as there will never be any optional information elements.

TAB. 6.3 – Short measurement report PDU (LIP new)

Time elapsed : Représente le temps approximatif depuis la dernière détermination de position (< 5 s, < 5 min, < 30 min, pas disponible).

Type of additionnal data : Détermine si le champ *« reason for sending »* ou *« user defined data »* sera utilisé.

Reason for sending : Indique la raison pour laquelle l'information a été émise depuis l'entité chargée de la localisation.

User defined data : Format libre, n'importe quelle valeur de 0 - 255.

Il existe également un *« Long location report »* qui permet la demande d'accusé de réception ainsi que la diffusion d'informations supplémentaires. Voici la version A-GPS de ce paquet (tab. 6.4).

Information element	Length	Type	C/O/M	Value	Remark
PDU type	2	1	M	$[1]_2$	Long location message
PDU type extension	4	1	M	$[1100]_2$	Long measurement report
Time data	Variable	1	M		
GPS Measurement info.	101 - 956	1	M		
Aknowledgment request	1	1	M		
Type of additionnal data	1	1	M		
Reason for sending	8		C		See note 1
User defined data	8		C		See notes 1 and 2
Extended user defined data	Variable	5	O		See note 2
Location message reference	8	5	O		
Result code	8	5	O		
SDS type-1 value	16	5	O		
Status value	16	5	O		
Terminal or location identification	Variable	5	O		

NOTE 1 : This information element shall be present as defined by the Type of additional data information element.

NOTE 2 : The contents of this information element is outside the scope of the present document.

This PDU shall not include any any O-bit or M-bit in the coding as type 5 optional information elements do not use that feature and the total length of the underlying transport protocol shall indicate whether any or any more optional information elements follow.

TAB. 6.4 – Long measurement report PDU (LIP New)

Time data : Permet de représenter le temps approximatif depuis la dernière détermination de position comme précédemment ou plus précisément en jour_du_mois/heure/minute.

Extended user defined data : Format libre, n'importe quelle valeur de 0 - 255.

Location message reference : Numérotation du paquet de localisation (0 - 255).

Result code : Code de retour de l'opération (succès, erreur système, ressources insuffisantes...)

SDS type-1 : Pas d'application ici.

Status value : idem.

Terminal or location identification : Source de l'information de localisation ou identificateur dans le cas ou le paquet est envoyé depuis une autre adresse (par exemple celle du serveur de localisation).

6.4 Demander assistance GPS

Un autre problème se pose à présent : à l'initialisation, lors d'un déplacement ou après une période de mauvaise réception, le traqueur demande au serveur de géolocalisation l'envoi des données d'assistance GPS de manière à pouvoir se verrouiller rapidement sur les satellites. Voici la description d'un nouveau paquet LIP s'acquittant de cette tâche (tab 6.5).

Information element	Length	Type	C/O/M	Value	Remark
PDU type	2	1	M	$[1]_2$	Long location message
PDU type extension	4	1	M	$[1011]_2$	Request assistance data
Request/Response	1	1	M	$[0]_2$	Request
Terminal or location identification	Variable	5	O		See note 1

NOTE 1 : Original location information source or identifier in the case this PDU is sent to another address e.g. location server address.

This PDU shall not include any O-bit or M-bit in the coding as type 5 optional information elements do not use that feature and the total length of the underlying transport protocol shall indicate whether any or any more optional information elements follow.

TAB. 6.5 – Request assistance data (LIP new)

Il reste maintenant à définir la réponse du serveur. Toujours dans le même ordre d'idées, nous avons recours au protocole RRLP afin d'identifier les champs de données importants pour l'assistance (tab. 6.6).

	8	7	6	5	4	3	2	1
Octet 1	IEI							
Octet 2	Length indicator							
Octet 3	H	G	F	E	D	C	B	A
Octet 4	P	O	N	M	L	K	J	I
Octet 5 to Octet 8+2n	Satellite related data							

TAB. 6.6 – Requested GPS assistance data IE (RRLP)

Le détail des différents champs de données peut être consulté à l'annexe B. Voici donc la réponse du serveur à une demande d'assistance (tab. 6.7).

Information element	Length	Type	C/O/M	Value	Remark
PDU type	2	1	M	$[1]_2$	Long location message
PDU type extension	4	1	M	$[1011]_2$	Request assistance data
Request/Response	1	1	M	$[1]_2$	Response
GPS assistance data IE	64-96	1	M		
Terminal or location identification	Variable	5	O		See note 1

NOTE 1 : Original location information source or identifier in the case this PDU is sent to another address e.g. location server address.

This PDU shall not include any O-bit or M-bit in the coding as type 5 optional information elements do not use that feature and the total length of the underlying transport protocol shall indicate whether any or any more optional information elements follow.

TAB. 6.7 – Requested assistance data (LIP new)

6.5 Vérifier présence traqueur/implant

Pour mener à bien cette tâche, le *« Long location report PDU »* qui autorise l'inclusion de données utilisateur sera utilisé. Les champs d'information « Location data » et « Velocity data » étant obligatoires, ils contiendront une valeur nulle.

Afin d'indiquer au traqueur ou à l'implant qu'il s'agit d'une vérification de présence, nous utiliserons le champ *« Extended user defined area »* auquel nous affecterons la valeur $[1]_2$. L'accusé de réception comportera également ce code dans la zone de données utilisateur étendue. La norme autorise une

Information element	Length	Type	C/O/M	Value	Remark
PDU type	2	1	M	$[1]_2$	Long location message
PDU type extension	4	1	M	$[11]_2$	Long location report
Time data	Variable	1	M		
Location data	Variable	1	M	$[0]_2$	
Velocity data	Variable	1	M	$[0]_2$	
Aknowledgment request	1	1	M	$[1]_2$	
Type of additionnal data	1	1	M	$[1]_2$	User defined data
User defined data	8		C	$[1]_2$	= Check presence

TAB. 6.8 – Check presence request PDU (tracker ↔ implant)

longueur variable pour ce champ mais nous utiliserons uniquement 8 bits comme pour la *« User defined area »*.

Information element	Length	Type	C/O/M	Value	Remark
PDU type	2	1	M	$[1]_2$	Long location message
PDU type extension	4	1	M	$[100]_2$	Location report acknowledgment
Reserved	8	1	M	$[0]_2$	Reserved for result reasons
Extended user defined data	8	5	O	$[1]_2$	= Check presence

TAB. 6.9 – Check presence acknowledgement PDU (implant ↔ tracker)

Pour le rapport de présence au serveur de localisation, nous utiliserons le code $[10]_2$ pour indiquer que le traqueur/implant est présent et a donc répondu à l'appel, $[11]_2$ dans le cas contraire.

Information element	Length	Type	C/O/M	Value	Remark
PDU type	2	1	M	$[1]_2$	Long location message
PDU type extension	4	1	M	$[11]_2$	Long location report
Timed data	Variable	1	M		
Location data	Variable	1	M	$[0]_2$	
Velocity data	Variable	1	M	$[0]_2$	
Aknowledgment request	1	1	M	$[1]_2$	
Type of additionnal data	1	1	M	$[1]_2$	User defined data
User defined data	8		C	$[1X]_2$	= Check presence
Terminal or location identification	16	5	O		Tracking server

TAB. 6.10 – Presence report (tracker/implant → location server)

Information element	Length	Type	C/O/M	Value	Remark
PDU type	2	1	M	$[1]_2$	Long location message
PDU type extension	2	1	M	$[1]_2$	Location report acknowledgment
Reserved	8	1	M	$[0]_2$	Reserved for result reasons
Etended user defined data	Variable	5	O	$[1X]_2$	

TAB. 6.11 – Presence report acknowledgment (tracking server → tracker/implant)

6.6 Envoyer Alerte

Pour l'envoi de l'alerte, le code $[111]_2$ sera utilisé comme *« User defined data »*.

Information element	Length	Type	C/O/M	Value	Remark
PDU type	2	1	M	[1]	Long location message
PDU type extension	4	1	M	$[11]_2$	Long location report
Time data	Variable	1	M		
Location data	Variable	1	M	$[0]_2$	
Velocity data	Variable	1	M	$[0]_2$	
Aknowledgment request	1	1	M	$[1]_2$	
Type of additionnal data	1	1	M	$[1]_2$	User defined data
User defined data	8		C	$[111]_2$	= Send alert
Terminal or location identification	16	5	O		Tracking server

TAB. 6.12 – Send alert (tracker → implant)

Information element	Length	Type	C/O/M	Value	Remark
PDU type	2	1	M	$[1]_2$	Long location message
PDU type extension	4	1	M	$[100]_2$	Location report acknowledgment
Reserved	8	1	M	$[0]_2$	Reserved for result reasons
Extended user defined data	Variable	5	O	$[111]_2$	Alert

TAB. 6.13 – Alert acknowledgment (tracking server → tracker)

6.7 Modifier trigger

Ce paquet permet la modification ou l'ajout d'un trigger. Les triggers permettent de forcer l'émission des coordonnées sous certaines conditions.

L'expéditeur doit adresser ce paquet au serveur de suivi, en indiquant son adresse source dans *« terminal or location identification »*. Le serveur transfère la requête au traqueur/implant et renvoie l'accusé de réception au demandeur en plaçant l'adresse du traqueur/implant dans *« terminal or location identification »*.

Report type : Choix entre *« short »* et *« long location report »*.

Trigger definition : Définition du/des triggers avec des paramètres tels que

- one shot/recurrent
- intervalle de distance maximal
- intervalle de temps maximal
- approche d'un point déterminé...

xxx Accuracy : Ces champs permettent de fixer la précision de mesure désirée.

Maximum information age : Fixe le temps après lequel l'information de localisation est périmée. Passé ce délais, une nouvelle localisation doit-être effectuée.

Maximum response time : Fixe le temps maximum alloué au calcul de position avec la précision demandée par le traqueur ou l'implant. Passé ce délais, si la précision requise n'est pas atteinte, alors le rapport est émis avec une mention spéciale.

Request priority : Fixe la priorité du trigger.

Start time/Stop time : Le moment ou le/les triggers doivent être activés/désactivés.

L'accusé de réception consiste à répéter ces données. Le demandeur peut ainsi s'assurer de la validité des réglages. Il est également possible de supprimer des triggers ou d'en récupérer la liste. Les détails sur ces opération peuvent être consultés dans [6].

6.8 Demander Position

Ce paquet (voir tab. 6.15 page 51) est utilisé afin de demander la transmission immédiate des coordonnées. Le paquet doit être adressé au serveur de suivi et *« terminal or location identification »* doit contenir l'adresse du

Information element	Length	Type	C/O/M	Value	Remark
PDU type	2	1	M	$[1]_2$	Long location message
PDU type extension	4	1	M	$[110]_2$	Add/Modify trigger
Request/response	1	1	M	$[0]_2$	Request
Acknowledgement request	1	1	M		
Report type	2	5	M		
Terminal or location identification	Variable	5	O		See note 1
Trigger definition	Variable	5	O		Repeatable, see note 2
Direction of travel and direction of travel accuracy	Variable	5	O		See note 3
Horizontal position and horizontal position accuracy	Variable	5	O		
Horizontal velocity and horizontal velocity accuracy	Variable	5	O		See note 4
Location altitude and location altitude accuracy	Variable	5	O		See note 5
Maximum information age	7	5	O		
Maximum response time	7	5	O		
Request priority	2	5	O		See note 6
Start time	22	5	O		
Stop time	22	5	O		
Vertical velocity and vertical velocity accuracy	Variable	5	O		See note 5

NOTE 1 : Original location information source or identifier in the case this PDU is sent to another address e.g. location server address.

NOTE 2 : This trigger and information elements up to next trigger definition information element belong together. Each Trigger definition shall start a new set of parameters, if those parameters are needed.

NOTE_3 : If report type value is "Short location report preferred", then the accuracy definition of this information element has a limited usage due to the resolution of the Direction of travel information element.

NOTE 4 : If report type value is "Short location report preferred", then the horizontal velocity without horizontal velocity uncertainty indication is implied and this information element may not be used.

NOTE 5 : If report type value is "Short location report preferred", then this information element should not be used.

NOTE 6 : The request priority may be used to set trigger priority

This PDU shall not include any any O-bit or M-bit in the coding as type 5 optional information elements do not use that feature and the total length of the underlying transport protocol shall indicate whether any or any more optional information elements follow.

TAB. 6.14 – Add/Modify trigger request PDU

traqueur ou de l'implant. Les champs de données ont été décrits au point précédent.

Information element	Length	Type	C/O/M	Value	Remark
PDU type	2	1	M	$[1]_2$	Long location message
PDU type extension	4	1	M	$[1]_2$	Immediate location report
Request/response	1	1	M	$[0]_2$	Request
Report type	2	5	M		
Location information destination	Variable	5	O		See note 1
Terminal or location identification	Variable	5	O		See note 2
Direction of travel and direction of travel accuracy	Variable	5	O		See note 3
Horizontal position and horizontal position accuracy	Variable	5	O		
Horizontal velocity and horizontal velocity accuracy	Variable	5	O		See note 4
Location altitude and location altitude accuracy	Variable	5	O		See note 5
Maximum information age	7	5	O		
Maximum response time	7	5	O		
Vertical velocity and vertical velocity accuracy	Variable	5	O		See note 5

NOTE 1 : Shall be included if location information destination is different than the source address of this PDU.

NOTE 2 : Original location information source or identifier in the case this PDU is sent to another address e.g. location server address.

NOTE_3 : If report type value is "Short location report preferred", then the accuracy definition of this information element has a limited usage due to the resolution of the Direction of travel information element.

NOTE 4 : If report type value is "Short location report preferred", then the horizontal velocity without horizontal velocity uncertainty indication is implied and this information element may not be used.

NOTE 5 : If report type value is "Short location report preferred", then this information element should not be used.

This PDU shall not include any any O-bit or M-bit in the coding as type 5 optional information elements do not use that feature and the total length of the underlying transport protocol shall indicate whether any or any more optional information elements follow.

TAB. 6.15 – Immediate location request PDU

6.9 Conclusion

Ce chapitre a permis de mettre en évidence les champs de données du protocole LIP utilisés par le système. Une proposition d'implémentation A-GPS pour LIP a également été réalisée afin de satisfaire aux exigences fonctionnelles. Les champs de données dont le codage est laissé libre à l'utilisateur ont permis d'adapter le protocole à nos besoins.

Quatrième partie

Sécurité

Chapitre 7

Exigences et risques

7.1 Exigences

Tout d'abord, quelles sont les exigences de notre application ?

1. Protéger efficacement des données contre un accès non autorisé par des utilisateurs ou des tierces parties telles que les fournisseurs de services du réseau par exemple.
2. Ne pas réduire la précision ni les fonctionnalités du système de positionnement.
3. Permettre un traitement sûr par les entités autorisées de l'infrastructure telles que le serveur de localisation.
4. Disposer d'un mécanisme de sécurité suffisamment léger pour les systèmes embarqués du traqueur, de l'implant ou du terminal TETRA.

7.2 Attaques passives

Ce type d'attaque, ne modifiant pas de données sur le réseau, constitue notre première catégorie de risques. En raison de leur caractère passif, ces attaques sont difficiles à détecter. Elles sont d'autant plus faciles que le média sans-fil est difficilement maîtrisable.

7.2.1 L'écoute (eavesdropping)

Une personne mal intentionnée pourrait écouter le trafic de contrôle et de données. Les informations de contrôle peuvent servir à déterminer la to-

pologie du réseau, sa configuration. Le trafic de données peut contenir des informations plus détaillées que celles accessibles depuis le serveur de suivi.

7.2.2 L'analyse de trafic (traffic analysis)

L'analyse de trafic permet de voir les variations du nombre de paquets transmis entre certains noeuds ce qui pourrait révéler une activité particulière sur un relais TETRA.

7.3 Attaques actives

Ces attaques, plus facilement repérables car elles injectent ou altèrent des données du réseau, constituent notre seconde catégorie de risques. Elles sont cependant plus dangereuses pour le fonctionnement du réseau.

7.3.1 L'usurpation d'identité (masquerading)

Un attaquant pourrait se faire passer pour un des dispositifs portables (traqueur/implant) et renseigner de fausses informations au serveur de suivi.

7.3.2 Homme du milieu (man in the middle)

Considérons par exemple le traqueur et le serveur d'infrastructure TETRA. Cette technique consiste à se placer entre les deux composants et à se faire passer pour le serveur par rapport au traqueur et vice-versa. Cela permet de surveiller tout le trafic réseau entre le traqueur et le serveur, et de le modifier à sa guise pour l'obtention d'informations.

7.3.3 La répétition (replaying)

Une autre attaque possible est celle de la répétition de données émises par le traqueur/implant. Plus spécifiquement, pour les réseaux radio, il existe l'attaque *« wormhole »* littéralement « trou de ver » qui consiste à brouiller les transmissions d'un traqueur par exemple, à réacheminer les données et à les diffuser à un autre endroit.

Chapitre 8

La sécurité TETRA

L'interface sans-fil (le réseau hertzien entre le mobile et l'infrastructure TETRA) est très vulnérable aux écoutes illicites. Un système de communication moderne se doit donc de fournir une sécurité efficace. En général, la protection standard fournie par TETRA pour l'interface sans-fil est considérée comme suffisante mais il existe des applications (telles que la nôtre) où une sécurité accrue est nécessaire. TETRA est relativement flexible et autorise dans ce cas un chiffrement bout en bout.

8.1 Chiffrement de l'interface sans-fil

Dans ce cas, le trafic de contrôle ainsi que le le trafic utilisateur peut être sécurisé entre le mobile et l'infrastructure TETRA. Le chiffrement de la voix et des données est disponible aussi bien pour les modes point à point que point à multipoint. Différents algorithmes de chiffrement (propriétaires ou libres) sont autorisés. Le chiffrement du trafic de contrôle empêche l'écoute illicite et la découverte des correspondants d'une communication par l'attaquant. Le réseau ASTRID intègre ce type de sécurité.

8.1.1 Authentification utilisateur

Chaque terminal possède une clé secrète K qui lui est propre. Cette clé peut soit être programmée par le gestionnaire du réseau dans le terminal, soit être programmée dans une carte à puce (SIM), ou encore, entrée manuellement via le clavier alphanumérique du terminal TETRA. C'est le premier cas de figure qui s'applique au traqueur et à l'implant (programmation avant

mise en service).

Lors de l'initialisation du terminal, le centre d'authentification au sein de la SwMI dérive la clé de session KS à partir de la clé secrète K à l'aide du RS, le « Random Seed » et de l'algorithme TA1. La SwMI ou « Switching and Management Infrastructure » comprend les relais et serveurs de gestion TETRA. RS est un nombre aléatoire ou « vecteur » permettant d'initialiser le générateur pseudo-aléatoire cryptographique de TA11.

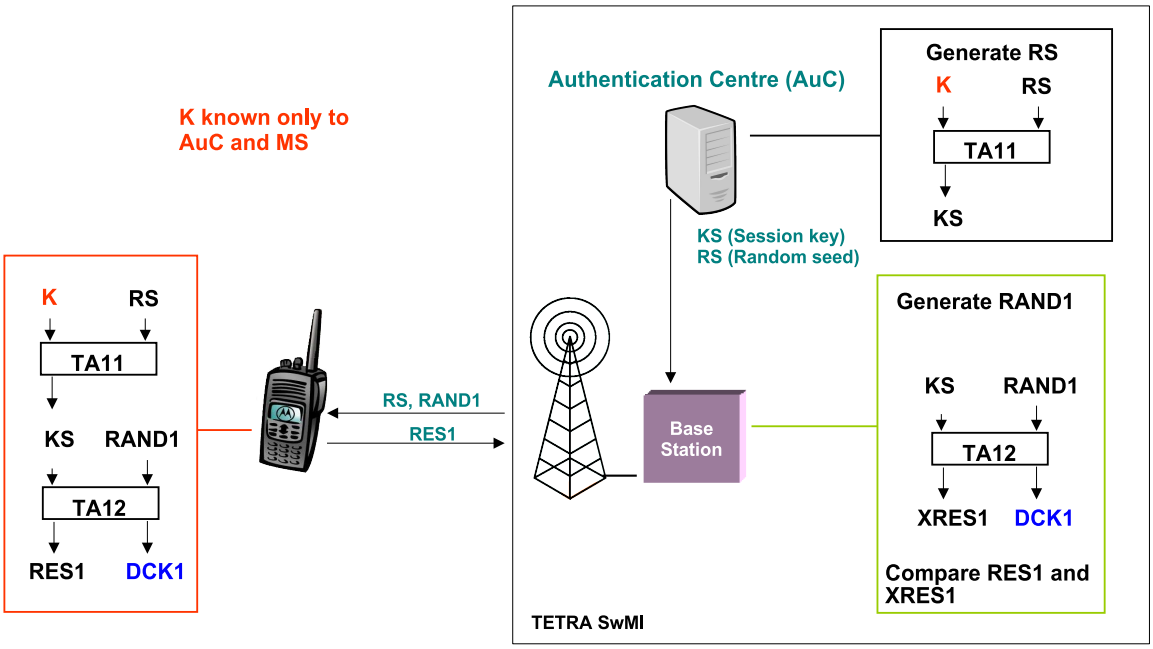

FIG. 8.1 – Authentification utilisateur

Cette clé de session est transmise à la station de base BS qui va générer un nombre aléatoire RAND1. Ce nombre, mélangé à KS dans l'algorithme TA12 fournira une clé de chiffrement dérivée DCK1 ainsi que la réponse attendue du terminal : XRES1.

RS et RAND1 sont transmis au terminal qui va générer KS avec le même algorithme TA11 que le centre d'authentification. Il calculera ensuite avec KS et RAND1 la réponse RES1 et la clé de chiffrement dérivée DCK1 au moyen l'algorithme TA12 équivalent à celui de BS.

La réponse RES1 sera renvoyée au contrôleur qui la comparera avec la réponse attendue XRES1. Si RES1 = XRES1 alors l'utilisateur est authentifié.

8.1.2 Authentification infrastructure

L'authentification de l'infrastructure par un utilisateur est réalisée de la même manière qu'au point précédent en inversant les rôles du vérificateur et du vérifié. C'est le terminal qui générera RAND2 et la réponse attendue XRES2. BS renverra la réponse RES2 et le terminal pourra ainsi la comparer avec XRES2. Une clé de chiffrement dérivée DCK2 sera également générée par ce processus. Les algorithmes sont cependant différents du point précédent et cela devrait être également le cas de la clé de session KS'.

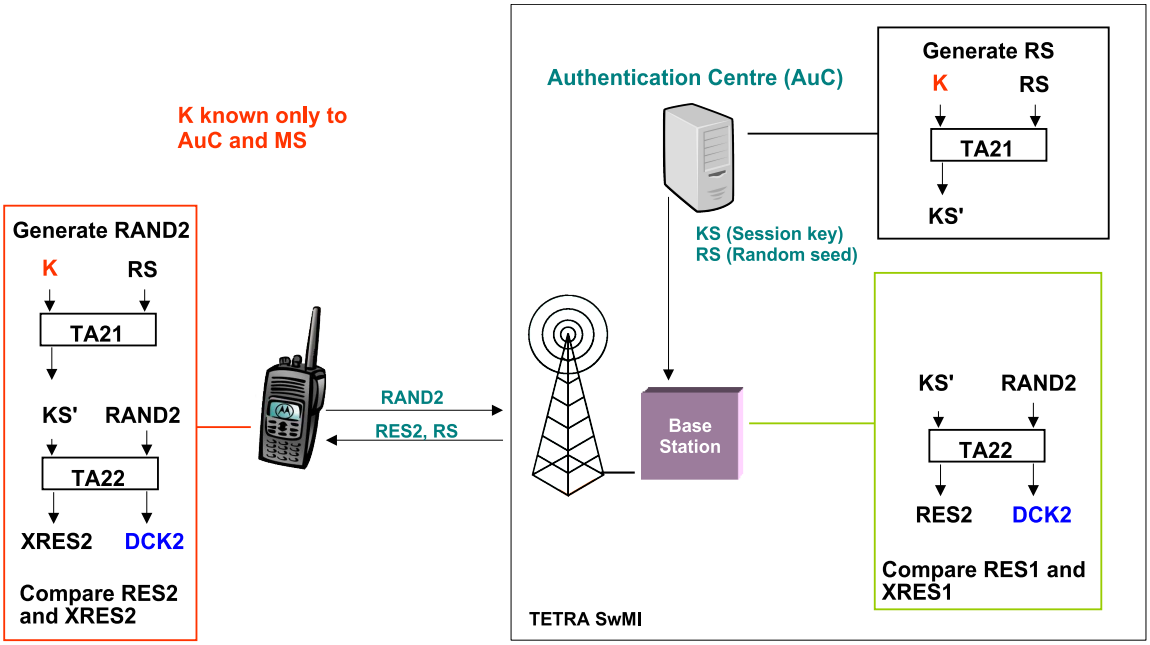

FIG. 8.2 – Authentification infrastructure

8.1.3 Les différentes clés

DCK (Derived Cipher Key) Cette clé est dérivée lors de la procédure d'authentification. Elle est utilisée pour chiffrer la liaison individuelle entre un terminal et le réseau. Elle fournit donc une authentification implicite lors d'une communication. Elle sert pour le chiffrement de l'envoi et de la réception de données.

CCK (Common Cipher Key) Elle est générée par le SwMI et distribuée chiffrée au moyen de la DCK à chaque terminal. Cette clé est utilisée comme modificateur de la GCK pour les communications de groupe (voir point suivant).

GCK (Group Cipher Key) Elle est générée par le SwMI et distribuée chiffrée au moyen de la DCK à chaque terminal. Elle n'est jamais utilisée directement sous cette forme. Elle est combinée avec la CCK (qui diffère pour chaque station de base ou relais) pour former la *« Modified GCK »* (MGCK) qui sera utilisée dans une communication de groupe.

SCK (Symetric Cipher Key) La SCK est une clé prédéterminée qui peut être utilisée sans authentification préalable. Elle est « statique » dans le sens où elle n'est pas modifiée lors de la phase d'authentification. Il peut y en avoir jusqu'à 32 pour chaque identifiant TETRA (ITSI). Elles peuvent être distribuées de la même manière que les GCK. Elles peuvent être utilisées pour le chiffrement du mode direct (point à point) où elles constituent également un moyen d'authentification explicite. Certaines implémentations TETRA les utilisent pour le chiffrement des communications individuelles et de groupe en multipoint. Il est possible d'utiliser les SCK comme alternative aux DCK et CCK en cas de problème. Utilisées en mode direct, les SCK sont groupées de telle manière à avoir plusieurs de ces clés associées pour un groupe de discussion. Ceci permet à un terminal d'utiliser une clé pour la transmission et les autres pour la réception.

8.2 Chiffrement bout en bout

Ce service peut être implémenté de différentes manières ce qui autorise une certaine flexibilité face aux besoins spécifiques des utilisateurs. Le standard TETRA laisse donc beaucoup de liberté concernant l'implémentation de ce type de sécurité. Le chiffrement de l'interface sans-fil est indépendant du chiffrement bout en bout. C'est-à-dire que des données chiffrées avec cette technique le seront à nouveau sur l'interface sans-fil. Donc, un service invoqué sans chiffrement bout en bout sera quand même sécurisé sur l'interface sans-fil si cette sécurité est déployée sur le réseau.

La figure 8.3 représente la portée des deux types de sécurité dans le réseau

TETRA. On peut remarquer que le chiffrement de l'interface sans-fil porte uniquement sur la partie hertzienne alors que le chiffrement bout en bout assure la sécurité sans discontinuité de l'émetteur au récepteur.

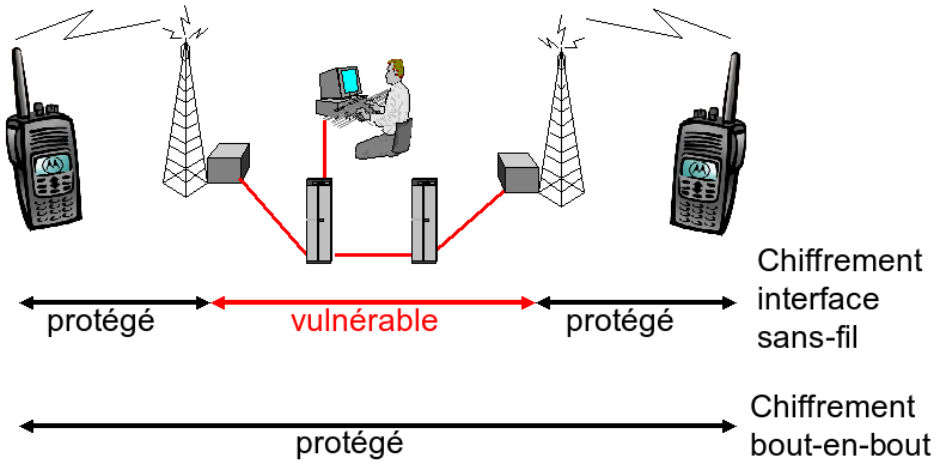

FIG. 8.3 – Sécurité TETRA

Chapitre 9

Contre-mesures

Dans ce chapitre, un état de l'art des techniques de sécurité spécifiques aux réseaux de géolocalisation sera réalisé. Les méthodes les plus simples seront énoncées en premier et pourront être intégrées au sein de méthodes plus évoluées.

9.1 Réduction de la précision

Une première approche, relativement simple, consiste à réduire la résolution spatiale et temporelle des informations de localisation [20]. Cependant la diminution de la précision des informations de localisation n'est pas compatible avec les besoins de notre application (point 2 des exigences). De toute manière, la protection liée à l'imprécision introduite est relativement limitée.

9.2 Utilisation de pseudonymes

Cette technique consiste à attribuer aux utilisateurs un identifiant sans lien direct avec leur véritable identité. Il suffit de communiquer les pseudonymes aux entités autorisées afin qu'elles soient capables de lier les données avec une identité réelle. Les fournisseurs de service ne peuvent donc pas lier des données à une identité bien qu'ils aient accès à ces données.

Un attaquant pourrait analyser les données de localisation qui pourraient révéler la véritable identité de l'utilisateur au travers de ses habitudes de déplacement, lieu de travail ou de résidence. La parade consiste alors à changer les pseudonymes après un certain temps.

9.3 Zones d'application

Dans certains systèmes, les utilisateurs utiliseront les services de localisation uniquement à certains endroits appelés zones d'application [21]. Entre ces zones se trouvent des zones de mélange où les utilisateurs n'ont souscrit à aucune application. Cette technique de sécurité repose également sur l'utilisation de pseudonymes. L'utilisateur qui rentre dans une zone de mélange prend un nouveau pseudonyme. Comme les applications ne reçoivent aucune information de localisation des utilisateurs présents de cette zone, il n'est pas possible de lier un utilisateur sortant à un utilisateur entrant ni même à un utilisateur présent dans la zone de mélange.

Ce procédé diminue la couverture du système de localisation en le confinant à un ensemble de petites zones ce qui est en contradiction avec le point 2 des exigences.

9.4 La transformation de coordonnées

Une transformation de coordonnées [22] est une application (dans le sens mathématique du terme) qui convertit n'importe quel point d'un système de coordonnées A en un autre point dans un système de coordonnées B.

Soit $\overrightarrow{c_{p,A}}$ les coordonnées d'un point $\overrightarrow{p}$ dans le système de coordonnées k_A et $\overrightarrow{c_{p,B}}$ les coordonnées du point $\overrightarrow{p}$ dans k_B, alors la transformation $t_{B,A}(\overrightarrow{x})$ converti les coordonnées de k_A vers k_B :

$$\overrightarrow{c_{p,B}} = t_{B,A}(\overrightarrow{c_{p,A}})$$

A la figure 9.1 la fonction de transformation $t_{B,A}(\overrightarrow{x})$ est représentée pour une question de simplicité par une unique translation bi-dimenssionelle :

$$t_{B,A}(\overrightarrow{x}) = \overrightarrow{x} + \overrightarrow{d_{B,A}}$$

On pourrait aussi utiliser une transformation qui serait une composition arbitraire de rotations et de translations :

- rotations : $t_{A,B}(\overrightarrow{x}) = R_{A,B}.\overrightarrow{x}$
- translations : $t_{A,B}(\overrightarrow{x}) = \overrightarrow{x} + \overrightarrow{d_{A,B}}$

$\overrightarrow{d_{A,B}}$ étant un vecteur de translation. Chaque transformation à les propriétés suivantes :

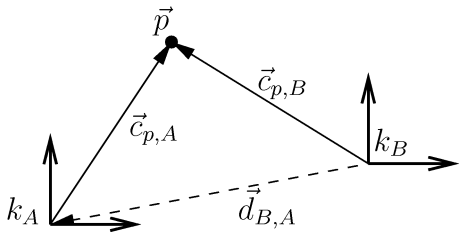

FIG. 9.1 – Représentation d'un point dans deux systèmes de coordonnées

1. $t_{B,A}(\overrightarrow{x})$ est bijective, c'est-à-dire qu'il existe une transformation inverse $t^{-1}_{B,A}(\overrightarrow{x}) = t_{A,B}(\overrightarrow{x})$
2. $t_{B,A}(\overrightarrow{x})$ préserve les distances et les angles entre les points
3. La composition de ces transformations peut être représentée par une transformation consistant en seulement une rotation et une translation $t_{C,A}(\overrightarrow{x}) = t_{C,B}(t_{B,A}(\overrightarrow{x})) = R_{C,A}.\overrightarrow{x} + \overrightarrow{d_{C,A}}$

La propriété 1 garantit que l'on peut retrouver la position originale par transformation inverse. Grâce à la propriété 2, il est possible de calculer les distances entre deux points sans connaître les transformations. La propriété 3 permet de diffuser la composition de deux transformations sans qu'il soit possible d'en déduire les transformations originales.

Un attaquant pourrait analyser des données de localisation et essayer de détecter des canevas (par ex : routes, bâtiments...) qu'il pourrait faire correspondre à des structures connues. Une solution consiste à changer fréquemment le système de coordonnées.

9.5 Le chiffrement de données

L'approche classique consiste à chiffrer les données de localisation dès leur émission. Les clés de chiffrement/déchiffrement sont mises à la disposition d'utilisateurs et services (serveurs de localisation, de suivi) autorisés. Dans le cas du chiffrement bout-en-bout, les données sont chiffrées tout au long de la transmission jusqu'au destinataire final. Les intermédiaires (services réseau) n'ont donc pas accès aux données. Un marqueur temporel ou un nombre aléatoire à usage unique peut être utilisé pour éviter les attaques de type répétition.

9.6 Packet leashes

En utilisant des *« packet leashes »* [23], ou littéralement « paquet en laisse », il est possible de détecter et d'éviter les attaques de type *« Wormhole »*. Ce procédé consiste à ajouter de l'information géographique *« geographical leashes »* ou temporelle *« temporal leashes »* à un paquet de manière à limiter la distance maximale qu'il peut parcourir ou sa durée de vie. Ce mécanisme n'assure pas la confidentialité de l'information qui peut alors être chiffrée à l'aide d'autres algorithmes.

Chapitre 10

Solution de sécurité

La technique retenue pour la sécurité de l'application est celle de la cryptographie facilitée par les mécanismes bout en bout de TETRA en plus du chiffrement par défaut de l'interface sans-fil sur le réseau ASTRID. A cela s'ajouteront l'utilisation de pseudonymes, les marquages temporels et les packet leashes.

10.1 Sécurité bout en bout

Afin d'utiliser la sécurité bout en bout de TETRA, le traqueur et l'implant posséderont tous deux une clé principale CP programmée lors de la mise en service et stockée de manière sûre. Cette clé permettra au serveur de suivi de transférer la clé de service CS chiffrée au traqueur/implant au moyen d'un algorithme de cryptographie symétrique. La cryptographie symétrique est choisie par rapport à la cryptographie asymétrique ou de clé publique en raison des capacités de calcul et de batteries limitées du traqueur et surtout de l'implant. C'est de plus, le système utilisé par la sécurité bout en bout TETRA.

La clé de service CS sert de paramètre à la fonction de génération de flux de clés GFC. Le second paramètre de cette fonction est VI, un vecteur d'initialisation que l'on fera varier sur base d'horloge pour éviter les attaques de type répétition.

Le flux de clés FC sert à chiffrer le message clair M à l'aide de la fonction Fl. $F1^{-1}$ réalise l'opération inverse au niveau du récepteur en combinant le message chiffré MC et FC.

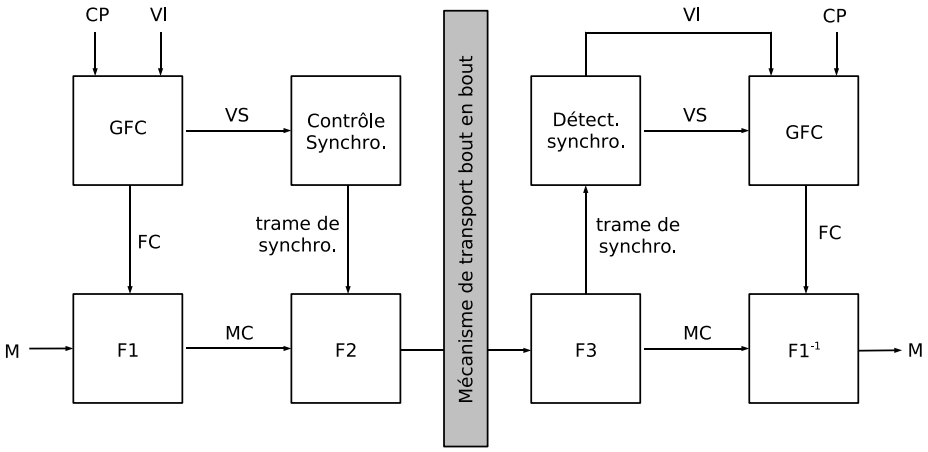

FIG. 10.1 – Principe du bout en bout TETRA

La valeur de synchronisation VS sert, avec l'aide de la fonction de contrôle de synchronisation à générer une trame de synchronisation. La fonction F2 se chargera de remplacer un demi slot de MC avec la trame de synchronisation.

La fonction F3 est chargée de détecter cette trame et de l'envoyer à la fonction de détection de synchronisation. Grâce à cette dernière, la fonction GFC recevra le VI et les VS identiques à celles de l'expéditeur. Les identifiants de l'utilisateur seront codés à l'aide de pseudonymes et l'utilisation d'un marquage temporel permettra d'éviter les attaques de type répétition.

10.2 Détection « Wormhole »

Afin de contrer ce type d'attaque, nous aurons recours aux *« temporal leashes »* (voir section 9.6 page 66). Les cas typiques de cette attaque dans notre application sont :

- Les données de l'implant sont relayées dans le cas du lien local avec le traqueur.
- Lorsque le traqueur n'est pas en mesure de recevoir les signaux GPS, ses données peuvent être relayées. Dans le cas contraire, il y aurait incohérence entre les données GPS et la mesure de position via TDOA, l'attaque serait donc vite repérée.
- Suite à la perte du traqueur, lorsque l'implant est directement relié au réseau TETRA, les données de ce dernier peuvent également être relayées.

Grâce aux informations de positionnement du traqueur, il est possible de connaître la distance que le message doit parcourir sur le réseau et, par conséquent, une borne supérieure du temps de parcours du paquet. Ce temps va dépendre du temps de propagation et du temps de traitement des noeuds intermédiaires. Les ondes radio circulant à la vitesse de la lumière, le temps de propagation sera très court.

Ce système requiert donc que les horloges des interfaces sans-fil soient synchronisées très précisément, de l'ordre de la microseconde voire nanoseconde. Grâce à l'utilisation du TDMA inhérente au réseau TETRA, cette précision peut être atteinte.

$$t_v = n.t_t + t_p + \triangle t$$

Le temps de validité t_v d'un paquet correspond à n noeuds intermédiaires multiplié par le temps de traitement t_t de ces noeuds (considéré comme équivalent) plus le temps de propagation t_p ainsi que l'écart maximal de synchronisation entre les horloges $\triangle t$.

Lors de l'émission d'un paquet, l'expéditeur devra renseigner le temps de l'émission t_e. Le récepteur comparera t_e à t_r, le temps de réception du paquet. Il pourra alors déterminer si le paquet à voyagé trop longtemps sur base du temps de propagation et des temps de traitement des noeuds intermédiaires.

Dans le cas du lien local entre le traqueur et l'implant, un intervalle de temps très court doit être fixé. Typiquement $2.t_p + t_e$ avec un t_e de l'ordre de 1 ns (représentant une distance de 3 m).

Conclusion

Les technologies émergentes de géolocalisation et des réseaux numériques hertziens laissent entrevoir de nombreuses applications nouvelles. L'objectif de ce travail est de proposer une solution de géolocalisation de personnes au travers du réseau ASTRID et plus généralement des réseaux TETRA.

ASTRID est un réseau numérique, dédié aux professionnels du secours et de la sécurité, implémentant la norme TETRA. Cette norme jouit d'une popularité grandissante en Europe et dans le monde, particulièrement dans le domaine des réseaux numériques professionnels.

De nombreuses applications sont possibles, mais la présente étude a été menée sur la surveillance électronique de condamnés, en raison des contraintes élevées illustrant bien ce système de géolocalisation.

Le dispositif utilisé actuellement par les autorités se compose d'un bracelet de cheville et d'un boîtier relié au réseau téléphonique. Cela permet uniquement de s'assurer de la présence du condamné dans le lieu qui lui a été assigné comme résidence. La solution proposée s'avère bien plus performante, car elle permet une localisation précise des personnes, à chaque instant, même en dehors de leur domicile. Grâce à cette solution, les autorités seront dotées d'un moyen de surveillance efficace tout en permettant aux condamnés de se réintégrer dans la vie active.

Pour atteindre cet objectif, des modifications doivent être apportées au protocole LIP. Ces modifications constituent une extension qui a été définie dans ce mémoire. Elle consiste principalement en l'ajout du support du GPS assisté et peut servir de référence à l'évolution officielle du protocole LIP au sein de l'ETSI.

En raison des exigences élevées de cette application, il sera possible, avec un effort limité, de l'adapter à d'autres cas d'utilisation comportant des contraintes équivalentes ou moindres (pompiers, police, malades...).

Ce travail constitue donc l'apport d'une nouvelle application intégrable à TETRA pour un coût relativement réduit. En effet, peu de changements sont nécessaires au niveau du réseau, l'application tirant au maximum profit de l'infrastructure logicielle et matérielle existante. Pour cette même raison, l'effort d'intégration est relativement limité.

Les points forts du système proposé résident dans sa disponibilité, sa précision et sa sécurisation. Premièrement, en raison de l'utilisation de différentes techniques de communication et de géolocalisation telles que TETRA, Argos, GPS, GPS différentiel et GPS assisté. Deuxièmement, grâce à une solution de sécurité présente à deux niveaux distincts. Au premier niveau, la sécurité est assurée par la couche TETRA elle-même. Au second niveau, la combinaison de différents mécanismes de sécurité permet de prévenir les attaques spécifiques aux réseaux de géolocalisation.

Les points faibles résident dans les limitations techniques actuelles, relatives à la miniaturisation des composants et plus spécifiquement de l'implant. L'utilisation trans-frontalière du système est également relativement limitée à l'heure actuelle. Néanmoins, plusieurs pays étrangers, en l'occurrence frontaliers, s'équipent progressivement en infrastructures TETRA.

Enfin, la consultation d'une commission éthique est indispensable, afin d'ouvrir un dialogue nécessaire pour définir le cadre d'utilisation de ce dispositif, respectant la vie privée.

Il reste également des questions en suspens. Par exemple, il convient d'étudier la montée en charge des réseaux TETRA. Dans le cas d'ASTRID, le réseau supporte potentiellement 40 000 terminaux. A l'heure actuelle, cette limite est loin d'être atteinte mais il clair que cela réduit le type et le nombre d'applications. Cette capacité pourrait néanmoins être étendue ultérieurement, la demande appelant l'offre. Il faut cependant préciser que la limite actuelle tient compte des terminaux pour communication vocale et que, en comparaison, le système proposé utilise une bande passante relativement limitée.

Un autre aspect nécessitant une étude complémentaire concerne la couverture du réseau. Est-elle suffisante pour un dispositif portable pouvant se trouver à l'intérieur de bâtiments ? Quels seraient les coûts d'une telle extension si elle s'avérait nécessaire ? Il convient cependant de nuancer cet aspect. En effet, dans le cadre d'une utilisation professionnelle (police, secours) un terminal TETRA à portée du réseau (à bord d'un véhicule par exemple) peut

servir de relais pour des utilisateurs situés dans une zone hors couverture.

Même si une réglementation en fixe le cadre légal, il faut également tenir compte des effets des rayonnements électromagnétiques sur les tissus biologiques, fonction du couple fréquence - puissance. Pour le traqueur, une comparaison peut être réalisée avec les GSM. Mais quels sont donc les effets de dispositifs, directement en contact avec des tissus biologiques tels que les implants ?

Finalement, cette étude ne représente qu'une partie du travail. La conception et la sécurisation des applications clientes, serveur et bases de données devront faire l'objet de développements ultérieurs.

Bibliographie

[1] Direction générale Exécution des Peines et Mesures, « Surveillance électronique ». Circulaire ministérielle n° 1746bis, Nov 2002.

[2] C. Defraigne, « Proposition de loi instaurant la surveillance électronique comme peine autonome ». Document législatif n° 3-266/1, Oct 2003.

[3] ASTRID, « All-round semi-cellular trunking radio communication system with integrated dispatchings ». `http://www.astrid.be`.

[4] ETSI, « Terrestrial trunked radio (tetra) ; voice plus data ; part 1 : General network design ». ETSI TS 300 392-1 v1.3.1, Jun 2005.

[5] ETSI, « European telecommunications standards institute ». `http://www.etsi.org`.

[6] ETSI, « Terrestrial trunked radio (tetra) ; voice plus data and direct mode operation ; part 18 : Air interface optimized applications ; subpart 1 : Location information protocol ». ETSI TS 100 392-18-1 v1.2.1, Dec 2005.

[7] Wikipedia, « Global positioning system ». `http://fr.wikipedia.org/wiki/Global_positioning_system`.

[8] ESA, « Galileo ». `http://www.esa.int/esaNA/galileo.html`.

[9] Wikipedia, « Differential gps ». `http://en.wikipedia.org/wiki/Differential_GPS`.

[10] ESA, « European geostationary navigation overlay service ». `http://www.esa.int/esaNA/egnos.html`.

[11] G. Djuknic et R. Richton, « Geolocation and assisted gps », *Computer*, vol. 34, p. 123–125, Feb 2001.

[12] P. Poiré, G. Duchâteau et M. Bodenstorfer, « Intermediate results of score, a project for a first operational 112 service using egnoss », *in ION GNSS 2005, Long Beach, California*, Sep 2005.

[13] Alcatel, « Location based services for the enhancement of working environment ». `http://liaison.newapplication.it`.

[14] Centre National d'Etudes spatiales (CNES), « Argos ». `http://www.cnes.fr/web/479-argos.php`.

[15] J. Pyrgies et J. Ramaekers, « A secure system to electronically track sex offenders », *in Infopole : "Tracking, Tracing et Objets communicants (tags, RFID, ...)", Namur, Belgium*, 2006.

[16] ETSI, « Terrestrial trunked radio (tetra) ; voice plus data (v+d) ; part 18 : Air interface optimized applications ; sub-part 2 : Part 18 : Air interface optimized applications ; assisted gps (a-gps) ». ETSI TS 100 392-18-2 v0.0.1. Not yet published.

[17] 3GPP, « 3rd generation partnership project ». `http://www.3gpp.org`.

[18] ETSI, « Digital cellular telecommunications system (phase 2+) ; location services (lcs) ; mobile station (ms) - serving mobile location centre (smlc) radio resource lcs protocol (rrlp) (3gpp ts 44.031 version 6.8.0 release 6) ». ETSI TS 144 031 V6.8.0, Jul 2005.

[19] ETSI, « Digital cellular telecommunications system (phase 2+) ; location services (lcs) ; base station system application part lcs extension (bssap-le) (3gpp ts 49.031 version 6.5.0 release 6) ». ETSI TS 149 031 V6.5.0, Jul 2005.

[20] M. Gruteser et D. Grunwald, « Anonymous usage of location-based services through spatial and temporal cloaking. », *in MobiSys*, 2003.

[21] A. Beresford et F. Stajano, « Location privacy in pervasive computing », *Pervasive Computing, IEEE*, vol. 2, p. 46–55, Jan-Mar 2003.

[22] A. Gutscher, « Coordinate transformation - a solution for the privacy problem of location based services ? », *in Parallel and Distributed Processing Symposium, 2006. IPDPS 2006. 20th International*, p. 7pp., 25-29 April 2006.

[23] Y.-C. Hu, A. Perrig et D. Johnson, « Packet leashes : a defense against wormhole attacks in wireless networks », *in INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and*

Communications Societies. IEEE, vol. 3, p. 1976–1986, 30 March-3 April 2003.

Annexe A

GPS Measurement information element

This is an excerpt from the 3GPP specification [18], pages 47 - 51.

The purpose of the GPS Measurement Information element is to provide GPS measurement information from the MS to the SMLC. This information includes the measurements of code phase and Doppler, which enables the network-based GPS method where position is computed in the SMLC. The proposed contents are shown in table A.1, and the individual fields are described subsequently. See also Figure A.1 for an illustration of the relation between some of the fields.

Information element	**Length**	**Occurence**	**C/O/M**	**Resolution**	**Range**	**Unit**
Reference Frame	16	1	O	—	1 - 65535	ms
GPS TOW	24	1	M	1 ms	0 - 14399999	ms
# of Satellites (N_SAT)	4	1	M	—	1-16	—
Measurement parameters	57	N_SAT	M	see tab. A.2		

TAB. A.1 – GPS Measurement Information element content (RRLP)

This element is included in the Measure Position Response component if the network has requested the mobile to perform mobile-assisted location measurements using a GPS location method. Following fields are repeated a number of times told in Number of E-OTD/GPS Measurement Sets field if Multiple Sets element is included. If Multiple Sets element is not included,

the default value for sets is one (i.e. the following fields are present only once).

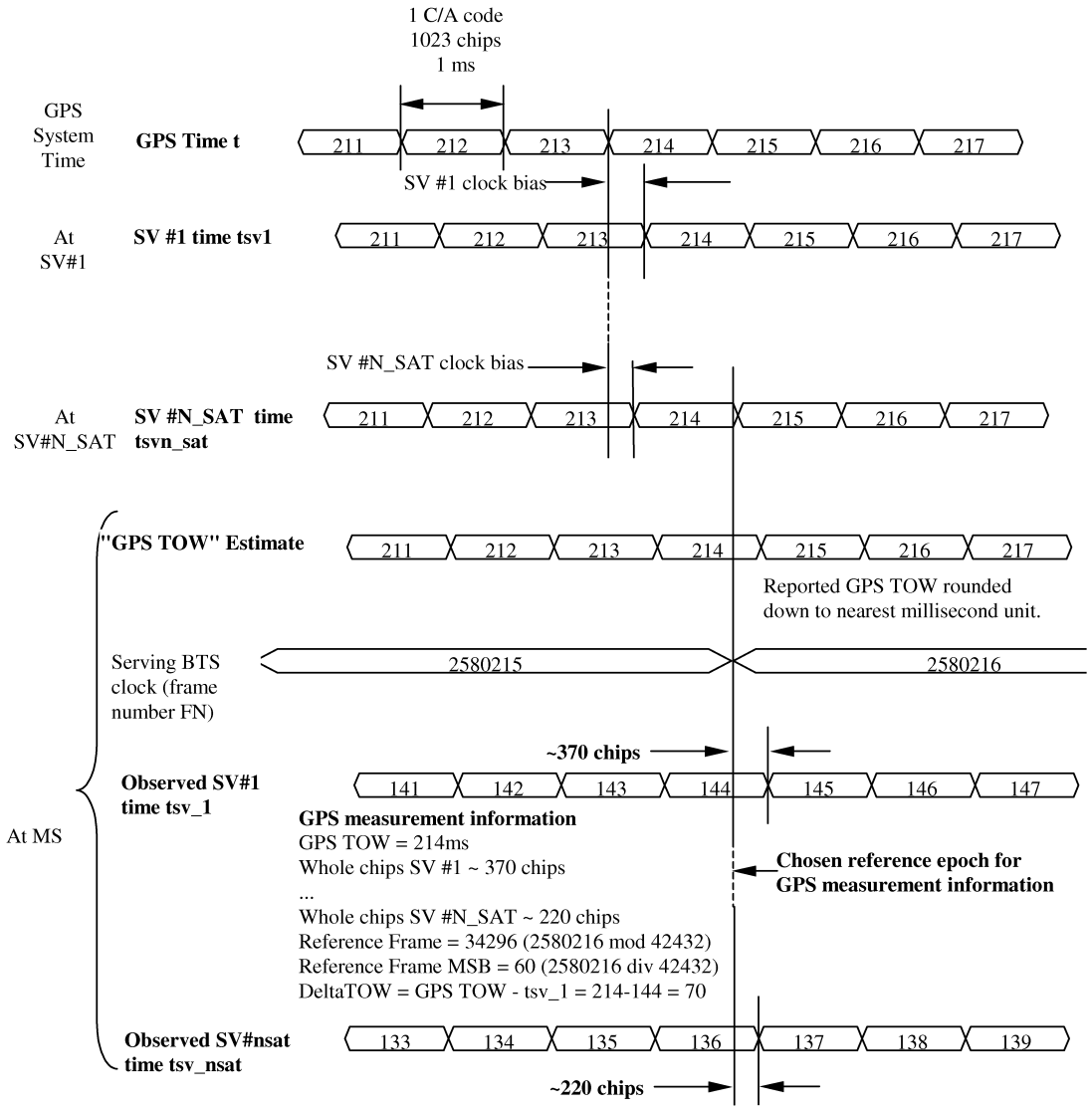

FIG. A.1 – Exemplary definitions of GPS measurement information fields.

Reference Frame This field is optional. Note that expected values for Reference Frame are in range 0 - 42431. If Reference Frame and GPS Time Assistance Measurements both are included in the RRLP Measure Position Response, the code phase measurements shall be aligned with the reported

GSM frame boundary observed by the MS at that time, as indicated in A.1. The time of the Reference Frame boundary is as observed by the MS, ie without Timing Advance compensation.

GPS TOW This field specifies the GPS TOW for which the location estimate is valid, rounded down to the nearest millisecond unit.This field is mandatory.

# of Satellites (N_SAT) Number of Measurements. This field specifies the number of measurements for which measurements satellites are provided in the component. This value represents the number of satellites that were measured by the MS. This value of N_SAT determines the length of the payload portion of the component. Typical range for N_SAT is four to a maximum of 12. This field is mandatory and occurs once per set.

Measurement Parameters This field contains information about the measurements of code phase and Doppler, which enables the network-based method where position is computed in the SMLC. This field is mandatory and occurs N_SAT times per message.

Information element	Length	Resolution	Range	Unit
Satellite ID	6	—	0 - 63	—
C/N_o	6	1	0 - 63	dB-Hz
Doppler	16	0.2	±6553.6	Hz
Whole Chips	10	1	0 - 1022	chips
Fractional Chips	11	2^{-10}	0 - (1 -2^{-10})	chips
Multipath Indicator	2	see tab. A.3		
Pseudorange RMS Error	6	3 bit mantissa 3 bit exp	0.5 - 112	m

TAB. A.2 – Measurement parameters field contents

Satellite ID This field identifies the particular satellite for which the measurement data is valid. This values 0 - 63 represent satellite PRNs 1 - 64, respectively.

C/N_0 This field contains the estimate of the carrier-to-noise ratio of the received signal from the particular satellite used in the measurement. It is

given in whole dBs and has a range of 0 to 63. Typical levels observed by MS-based GPS units will be in the range of 20 dB to 50 dB.

Doppler This field contains the Doppler measured by the MS for the particular satellite signal. This information can be used to compute the 3-D velocity of the MS. The Doppler range is sufficient to cover the potential range of values measured by the MS.

Whole Chips This field contains the whole value of the code-phase measurement made by the MS for the particular satellite signal at the time of measurement, in units of 1 GPS chip in the range from 0 to 1022 chips, where increasing binary values of the field signify increasing measured pseudoranges. The code phase measurement is divided into two fields, 'Whole Chips' and 'Fractional Chips'.

Fractional Chips This field contains the fractional value of the code-phase measurement made by the MS for the particular satellite signal at the time of measurement. The resolution of the fractional portion is approximately 0,3 m. NOTE : The actual ASN.1 coding of this field reserves 11 bits for legacy compatibility. Only the 10 least significant bits are actually required to code the values (0..1023)

Multipath Indicator This field contains the Multipath Indicator value. This parameter is specified according to the representation described in table A.3 Range : 0 - 3.

Value	Multipath Indication
00	Not measured
01	Low, MP error $<$ 5m
10	Medium, 5m $<$ MP error $<$ 43m
11	High, MP error $>$ 43m

TAB. A.3 – Multipath indicator values and associated indications

Pseudorange RMS Error This field contains a Pseudorange RMS Error value. Range : 0,5 m to 112 m NOTE : This parameter is specified according to a floating-point representation as described in Table A.4.

Index	**Mantissa**	**Exponent**	**Floating-Point value, x_i**	**Pseudorange value, P**
0	000	000	0.5	P < 0.5
1	001	000	0.5625	0.5 <= P < 0.5625
|	x	y	0.5 * (1 + x/8) * 2^y	x_{i-1} <= P < x_i
62	110	111	112	104 <= P < 112
63	111	111	—	112 <= P

TAB. A.4 – Pseudorange RMS error representation

Annexe B

GPS Assistance data

This is an excerpt from the 3GPP specification [19], pages 31 - 33.

This is a variable length information element identifying the GPS assistance data requested for an MS.

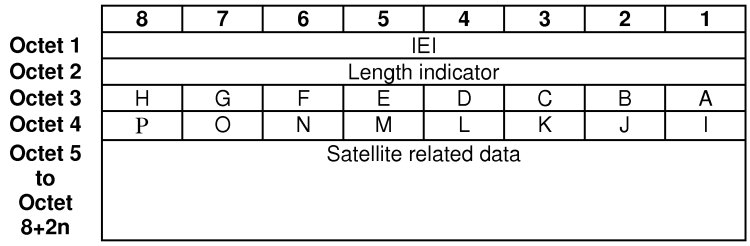

FIG. B.1 – Requested assistance data

IEI (octet 1) Information Element Identifier is $[\ 01001011\ ]_2$ in this case. The most significant bit is bit 8.

Length Indicator (octet 2) The most significant bit is bit 8. The length indicator defines the total number of octets after length indicator.

Octet 3

bit A Almanac

0 : Almanac is not requested

1 : Almanac is requested

bit B UTC Model

0 : UTC Model is not requested

1 : UTC Model is requested

bit C Ionospheric Model

0 : Ionospheric Model is not requested

1 : Ionospheric Model is requested

bit D Navigation Model

0 : Navigation Model is not requested - octets 5 to 8+2n are not present

1 : Navigation Model is requested - octets 5 to 8+2n are present

bit E DGPS Corrections

0 : DGPS Corrections are not requested

1 : DGPS Corrections are requested

bit F Reference Location

0 : Reference Location is not requested

1 : Reference Location is requested

bit G Reference Time

0 : Reference Time is not requested

1 : Reference Time is requested

bit H Acquisition Assistance

0 : Acquisition Assistance is not requested

1 : Acquisition Assistance is requested

bit I Real-Time Integrity

0 : Real-Time Integrity is not requested

1 : Real-Time Integrity is requested

bits J through P are Spare bits

At least one of bits A, B, C, D, E, F, G, H or I, shall be set to the value "1".

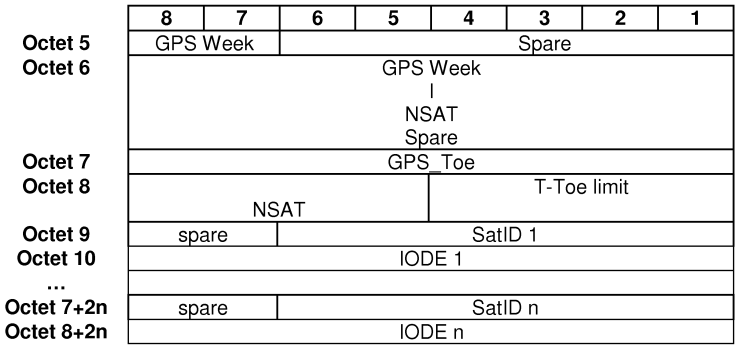

FIG. B.2 – Coding of Satellite Related Data

GPS Week (bits 7-8 octet 5 and octet 6) This field contains a 10 bit binary representation of the GPS Week of the assistance currently held by the MS. The most significant bit of the GPS Week is bit 8 in octet 5 and the least significant bit is bit 1 in octet 6.

GPS_Toe (octet 7) This field contains a binary representation of the GPS time of ephemeris in hours of the newest ephemeris set contained in handset memory (range 0-167).

NSAT (octet 8, bits 5-8) This field contains a binary representation of the number of satellites to be considered for the current GPS assistance request. If the MS has no ephemeris data, this field shall be set to zero. If the MS has ephemeris data whose age exceeds the T-Toe limit, this field may be set to zero. If the SMLC receives a zero value for this field, it shall ignore the GPS Week and GPS_Toe fields and assume that the MS has no ephemeris data.

T-Toe limit (octet 8, bits 1-4) This field contains a binary representation of the ephemeris age tolerance of the MS to the network in hours (range 0- 10).

SatID x (x = 1,2, ... n) (octet 7 + 2x, bits 1-6) This field is present only if NSAT exceeds zero and contains a binary representation of the identity of a satellite for which the assistance request is applicable. The number of satellite fields is indicated in the field NSAT.

IODE x (x = 1,2, ... n) (octet 8 + 2x) This field is present only if NSAT exceeds zero and contains a binary representation of the Issue of Data Ephemeris held in the MS, which identifies the sequence number for the satellite x (x = 1, 2, ..., n). The SMLC shall derive the issue date and time for the IODE of each satellite x from the GPS Week and GPS_Toe fields (e.g. when a particular IODE value for a satellite x was issued more than once within the period of T-Toe limit).